STRENGTH THROUGH KNOWLEDGE: HOMELAND SECURITY SCIENCE AND TECHNOLOGY SETTING AND STEERING A STRONG COURSE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

OF THE

SELECT COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

OCTOBER 30, 2003

Serial No. 108–33

Printed for the use of the Subcommittee on Cybersecurity, Science, and Research and Development, and the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

97–415 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, Chairman

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, JR., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, Ranking Member
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT

MAC THORNBERRY, Texas, Chairman

PETE SESSIONS, Texas, Vice Chairman
SHERWOOD BOEHLERT, New York
LAMAR SMITH, Texas
CURT WELDON, Pennsylvania
DAVE CAMP, Michigan
ROBERT W. GOODLATTE, Virginia
PETER KING, New York
JOHN LINDER Georgia
MARK SOUDER, Indiana
JIM GIBBONS, Nevada
KAY GRANGER, Texas
CHRISTOPHER COX, California, *ex officio*

ZOE LOFGREN, California
LORETTA SANCHEZ, California
ROBERT E. ANDREWS, New Jersey
SHEILA JACKSON-LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
JIM TURNER, Texas, *ex officio*

CONTENTS

STATEMENTS

WITNESS

APPENDIX

MATERIALS SUBMITTED FOR THE HEARING RECORD

STRENGTH THROUGH KNOWLEDGE: HOMELAND SECURITY SCIENCE AND TECHNOLOGY SETTING AND STEERING A STRONG COURSE

Thursday, October 30, 2003

U.S. HOUSE OF REPRESENTATIVES,
SELECT COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND
RESEARCH AND DEVELOPMENT
Washington, D.C.

The subcommittee met, pursuant to call, at 4:15 p.m., in Room 210, Cannon House Office Building, Hon. Mac Thornberry [chairman of the subcommittee] presiding.

Present: Representatives Thornberry, Sessions, Linder, Granger, Cox (ex officio), Lofgren, Andrews, Etheridge, Lucas, Meek, and Turner (ex officio).

Mr. THORNBERRY. The subcommittee will come to order.

And let me thank you first, Doctor, for your patience with our unpredictable schedule around here.

I want to ask unanimous consent that all Members be able to offer opening statements into the record.

[The information follows:]

PREPARED STATEMENT OF THE HONORABLE ROBERT E. ANDREWS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

The government has a history of driving technology innovations, including the essential software development conducted with Defense Department funding that laid a foundation for today's Internet. It would be very unfortunate-indeed, counterproductive-if companies were reluctant to adopt promising security technologies produced by federal research. As you move forward with your research agenda, I hope you will support technology transfer licensing models that empower the private sector to improve upon the government's work and to commercialize the resulting technology.

PREPARED STATEMENT OF THE HONORABLE JIM GIBBONS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEVADA

Chairman Thornberry, thank you for bringing us together today for this hearing on the long-term research and development plans of the Department of Homeland Security (DHS). Thank you, Dr. Albright for coming to testify before the Committee.

The ability to bring together the brightest minds in America to work on the common cause of securing our homeland is one of the most important tasks that face us as a nation. We are in a war, not only with terrorists and terrorist organizations, but with states who would seek to profit off of the proliferation of weapons of mass destruction. In that vein, our technologies and brightest minds need to be able to defeat the most advanced WMD technologies while at the same time, we need to be able to defeat a single fanatic carrying box-cutters or a deadly disease. This is a daunting task, but the consequences of failure are too great.

As we saw on 9–11, our enemies will go after our vulnerabilities in any way they can. While these threats will be hard to predict and difficult to prioritize, I wanted to take this opportunity to mention a serious potential threat that I see on the horizon that I do not believe is being adequately planned for.

Currently, our nuclear plants and facilities have increased security in order to protect against a catastrophic attack against our nuclear facilities and infrastructure. However, in the not-so-distant future we will be confronted with a new nuclear security dilemma.

Unless we change our course, we will soon have the additional burden of protecting against attacks on the shipment of highly radioactive spent nuclear fuel from points across this country to Yucca Mountain. I think that bears repeating: We will be taking this highly radioactive nuclear fuel out of secure locations, putting it on trucks and trains and moving it cross-country through populated areas across America. As long as these shipments are an attractive target for terrorists, they will be vulnerable to an attack.

The key way to protect against this threat, from my perspective, is to not make these shipments in the first place . However, the Department of Energy continues to push forward with the Yucca Mountain license at any cost, so it is my responsibility to make sure we are prepared for this eventuality. As a result, at the very least, we need to make sure that the nuclear waste casks they will be shipped in are so ?hardened? that they will not make an attractive target.

The design for the Spent Fuel Packages that will be used to transport this waste is currently being reviewed by Sandia National Labs for the Nuclear Regulatory Commission. If this study is properly performed, it can provide us with important information on the safety of these shipments and their vulnerabilities. However, I?m very concerned that the ?Package Performance Study? will not take into consideration the effects of deliberate acts of sabotage and terrorism.

The consequences of a successful attack on one of these canisters would be horrific. It is very clear to me that this is an issue that the Department of Homeland Security must address immediately, since now is the time to weigh in, while the Spent Fuel Packages are still being reviewed.

Thank you again Mr. Chairman and Dr. Albright. I look forward to working with you both to see that our homeland security science and technology needs are met.

Mr. THORNBERRY. I simply want to say that we had before this subcommittee Dr. McQueary back in May to talk to us about the beginning of the Science and Technology Directorate. We have subsequently had several sessions to try to understand better some of the key technologies dealing with homeland security, namely nuclear and radiological detection, first responder communications, and things like that. And we are interested today to get an update and status report both on how the Department is shaping up and conducting its business, but also Members may well want to explore some particular areas of technology.

And so with that, I also want to again thank Eric Fisher and his team from the Congressional Research Service for their support of this subcommittee, as well as my partner Ms. Lofgren. And I will yield to her at this point for any opening.

Ms. LOFGREN. Thank you. I have an opening statement that I will submit for the record. But I just wanted to note that it has been about 6 months since Dr. McQueary appeared before us, and he at that time mentioned seven specific areas for emphasis of the Directorate, and I am hoping that you can give us an update of where we are on all seven of those. I also hope that we can find out the progress of the MOU with NIST, how that is working.

Also, when Dr. McQueary appeared before us, I had an interest in what we were doing in terms of standards-setting on biometrics, and I am still interested in that and would like to be more knowledgeable about our efforts there.

Finally, I would just like to—I don't know how many more hearings we will have before we recess, but I would like to thank Mac

Thornberry for his leadership of his subcommittee this year. I think you have done a terrific job, and I think you have led the subcommittee well and with great fairness, and I really appreciate the work we have done together.

I also want to thank the staff of the subcommittee for their work during our inaugural year, and in particular Kim Kotlar and Margie Gilbert on your staff who are really very able, and on the Democratic side Jessica Herrera, and David Grannis and Dan Prieto, who have also done a very good job. And I think really this subcommittee is an example of what can happen when we work, and not on a bipartisan but really a nonpartisan basis. So it has been a pleasure being a part of that. And I yield back.

Mr. THORNBERRY. I thank the gentlelady for her comments, and certainly share them with regard to the staff.

[The information follows:]

PREPARED STATEMENT OF THE HONORABLE ZOE LOFGREN, RANKING MEMBER, SUBCOMMITTEE ON SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

Thank you Chairman Thornberry.

Almost 6 months ago, Under Secretary Dr. Charles E. McQueary of the Department of Homeland Security's Science and Technology Directorate testified before this subcommittee. It was the first hearing held by this subcommittee and it marked the beginning of our look into the work being done at the Department of Homeland Security.

At that time, Dr. McQueary was new to the job, and he spoke about his priorities for the S&T Directorate.

In his testimony, Dr. McQueary said "The most important mission for the Science and Technology Directorate is to develop and deploy cutting edge technologies and new capabilities, so that the dedicated men and women who have the awesome responsibility to secure our homeland could perform their jobs more effectively and efficiently."

He also mentioned 7 specific areas of emphasis for the Directorate. These included the following:

1. Develop and deploy state-of-the art, high-performance, low operating-cost systems to prevent the illicit traffic of radiological/nuclear materials and weapons into and within the United States.
2. Provide state-of-the art, high-performance, low operating-cost systems to rapidly detect and mitigate the consequences of the release of biological and chemical agents.
3. Provide state-of-the art, high-performance, low operating-cost systems to detect and prevent illicit high explosives transit into and within the United States
4. Enhance missions of all Department operational units through targeted research, development, test and evaluation (RDT&E), and systems engineering and development.
5. Develop and provide capabilities for protecting cyber and other critical infrastructures.
6. Develop capabilities to prevent new-technology as a surprise weapon by anticipating emerging threats.
7. Develop, coordinate and implement technical standards for chemical, biological, radiological, and nuclear (CBRN) non-medical countermeasures.

Mr. Chairman, Dr. McQueary proposed an ambitious agenda at that first hearing and the Members of this subcommittee were willing to give the Directorate some time to organize.

Now that the Directorate has had 6 months to get up and running, I think this is an appropriate time to review what has been accomplished thus far, and what has yet to be done.

Today we will hear from Dr. Penrose (Parney) C. Albright, Assistant Secretary for Plans, Programs, and Budget within the Science and Technology Directorate.

Dr. Albright, I look forward to hearing about the progress that has been made since we heard from Dr. McQueary.

I hope you will take some time today to discuss the status of Dr. McQueary's seven areas of emphasis.

In addition, I would like you to address some other issues that I addressed to Dr. McQueary last spring and I hope you will take some time today to discuss the following:

1. How is the Memorandum of Understanding (MOU) with the Department of Commerce's Technology Administration's National Institute of Standards and Technology (NIST) working? Do we need to be looking at any particular issues that have arisen out of this agreement, particurly in the area of ensuring that the funding needed to engage in some of this new cooperation is available?.
2. What steps have been undertaken and or being undertaken to engage the private sector in the development of new technologies and strategies we will need in the future, both short-term and long-term?
3. What has the Department of Homeland Security been doing in the area of biometrics? Should we being doing more and are there any challenges that you have encountered thus far that this subcommittee should be aware of?

Before I conclude, I want to note that this is likely to be the last hearing this subcommittee will hold before Congress adjourns for the year. I want to take just a minute to thank my colleague Mac Thornberry for his leadership of this subcommittee this year. Mac is a smart and able public servant, and he has led this subcommittee in a fair and bipartisan manner. I greatly look forward to continuing our work in 2004.

I also want to thank the staff of the Cybersecurity subcommittee for their work throughout our inaugural year. They have done terrific work getting this subcommittee up and running. In particular, let me mention Kim Kotlar and Margie Gilbert on Mr. Thornberry's staff. And on the Democratic staff, let me thank Jessica Herrera, David Grannis and Dan Preito.

Mr. THORNBERRY. Dr. Albright, thank you for being with us. I would like to now turn to you for your statement. Again, our witness is Dr. Parney Albright, Assistant Secretary for Plans, Programs, and Budget in the Science and Technology Directorate of the Department of Homeland Security. You are recognized for your opening statement.

STATEMENT OF PENROSE (PARNEY) C. ALBRIGHT, PH.D., ASSISTANT SECRETARY FOR PLANS, PROGRAMS AND BUDGET, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. ALBRIGHT. Good afternoon, Chairman Thornberry, Congresswoman Lofgren, and other members of the subcommittee. I am pleased to be here with you today to report on the progress of the Science and Technology Directorate of the Department of Homeland Security, and report on the progress we are making in implementing Title III of the Homeland Security Act of 2002.

As you noted, Chuck McQueary, the Under Secretary for Science and Technology, did appear before this subcommittee on May 21st, and I am here to update you on the status of our efforts to build out the Directorate.

In its planning, the Science and Technology Directorate has been guided by the Homeland Security Act, current threat assessments, our understanding of existing capabilities or those that can be anticipated in the near term, and by the priorities outlined in the President's National Strategy for Homeland Security.

The Directorate's key missions are to address chemical, biological, radiological, nuclear, cyber and other emerging threats; to support the R&D needs of the Department; to organize and engage and sustain the resources of the national research and development community, private industry, academia, national and Federal laboratories in protecting the homeland.

Let me first talk about the progress we have made in operating some of our key offices within the Directorate. All the key offices of the Science and Technology Directorate needed to execute the missions that I just articulated are, in fact, operational. Directors with strong credentials have been appointed to each office, and we continue to add highly skilled technical, professional, and support staff.

The Office of Plans, Programs and Budgets, which is the office I direct, is, in fact, operating. I have organized this office into several portfolios that are in line with the scope of the Directorate's missions. These portfolios focus on countermeasures for chemical, biological, radiological, nuclear, cyber, and high-explosive threats, meeting the needs of our Federal, State, and local customers, and also developing standards to help Federal, State, and local agencies become smart buyers of homeland security technologies.

Directors are now in place for each of these portfolios, and we are continuing to build out our staff. The staff of each portfolio, their job is to serve as experts in their particular area and understand the activities and capabilities that exist in Federal agencies and across the broad research and development community, and to develop a strategic plan for their particular portfolio with near, mid, and long-range research and development activities.

In addition, I have staff that understands the threat from a technical perspective and is tasked with integrating the various portfolios into a coherent overall plan, with develop a corresponding budget, and monitoring its financial execution.

Finally, I am responsible for directing and executing the Directorate's implementation responsibilities for the SAFETY Act.

It is our good fortune to have Dr. David Bolka, who joined us last month as the Director of the Homeland Security Advanced Research Projects Agency, known as HSARPA. Dr. Bolka made significant contributions in advancing technical and scientific projects in his prior work with Lucent Technologies and Bell Labs.

HSARPA is the key external research funding arm of the S&T Directorate. Its office is engaged in private sector and research and development activities in support of our mission and our customers. HSARPA also conducts rapid prototyping efforts aimed at taking nearly off-the-shelf technologies and adapting them for rapid fielding of new capabilities.

HSARPA's first priority has been to initiate the development of the next generation of chemical and biological sensors and systems to meet anticipated threats under existing conditions. They have engaged the private sector in its first solicitations, seeking detection systems for chem and bio countermeasures. The interest and response from the private sector has been strong. We recently held a bidders' conference in Washington on September 29th that drew approximately 400 participants, and we have received more than 500 white papers as a result of the solicitation. We are now selecting the finalists who will be invited to submit full proposals, and expect to begin contract negotiations in January.

HSARPA also plans to issue shortly a series of solicitations to address radiological, nuclear, and high-explosive threats. These and other solicitations will seek to engage our Nation's research and de-

velopment community, including academia FFRDCs, nonprofits, and industry.

In fiscal year 2004, about 60 percent of our appropriation will go directly to the private sector through HSARPA or other S&T entities, with about 90 percent of these funds dedicated to near-term technologies that can be quickly developed.

In addition, we also are pleased to have Dr. Maureen McCarthy on board as a Director of Science and Technology's Office of Research and Development. Dr. McCarthy has served as chief scientist for the National Nuclear Security Administration and the Department of Energy, and was DOE's senior representative to the Homeland Security Transition Planning Office. In fact, she was my deputy as the Transition Planning Office was stood up. She leads the office as it strives to provide the Nation with an enduring capability in research, development, demonstration, testing and evaluation of technologies to protect the homeland.

The activities within the Office of Research and Development address the resources that can be brought to bear to better secure the homeland through the participation of universities, national labs, and Federal research centers. Directors have been appointed to lead efforts in each of these areas, and staff is being added rapidly.

We also have asked John Kubricky, and he is to join Science and Technology, and he arrived earlier this month as the Director of the Office of Systems Engineering and Development. Mr. Kubricky previously served as the advanced program development manager for Northrop Grumman, and he is leading the implementation and transition of large-scale or pilot systems to the field through a rapid, efficient, and disciplined systems engineering approach.

One of our key challenges in S&T is to evaluate a wide spectrum of military and commercial technologies so that rapid, effective, and affordable solutions can be transitioned to the Department's customers, to include first responders and Federal agencies. In some cases, for example, military technologies could be candidates for commercialization, but rigorous system engineering processes need to be applied to ensure a successful transition.

An example of this is our 2-year effort to reengineer technologies developed in the military so that they can be used for protecting civilian aircraft against a shoulder-fired missile threat.

Our Systems Engineering Office will identify and retire in a disciplined and efficient manner those risks associated with developing and fielding such technologies. In doing so, the office must view each technology through the prism of affordability, performance, and supportability, all critical to our end users. Products must be user-friendly, require little or no training, and consistently provide accurate results. So our Office of Systems Engineering will demonstrate and test solutions before they are released to the field, and will validate those solutions to assure that they meet user expectations.

Now, as I indicated earlier, a key mission of ours is to support the research and development needs of the operational directorates within the Department. Let me say a little bit about how we support, as an example, the Information Analysis and Infrastructure Protection Directorate. The Department is very aware that our critical cyberinfrastructure is an attractive target for our adversaries.

In support of the IA&IP activities in this area, S&T is creating a robust cybersecurity research and development capability aimed at addressing our cyber vulnerabilities and engaging, for example, in efforts that develop tools to make it easier to perform software patches or detect the insider threat. This effort will be executed through a cyber R&D center managed through HSARPA. A center director has been selected along with a deputy director, who is from, in fact, our IA&IP Directorate.

A draft research agenda has been developed, and we are now soliciting for a contractor to support the center's operation. The contractor will host the necessary public and private discussions on technical issues, and will further develop the research agenda around the issues identified.

We also support the IA&IP Directorate with research, assessments and guidance in evaluating threats and areas of vulnerability. We provide the technical understanding of the current and evolving threat and cutting-edge tools to help intelligence analysts organize and query their data and to connect the dots. We strive to better understand the vulnerabilities and risks to our infrastructure while providing policymakers with the information they need to efficiently allocate resources for their protection.

We have also established a National Biodefense Analysis and Countermeasure Center in support of our Title III responsibilities. The National Biodefense Analysis and Countermeasure Center, based at Fort Detrick, Maryland, is the hub within Homeland Security for research and operational capabilities to anticipate, prevent, respond to, and recover from current and next-generation biological threats to the American people and our agricultural system. It has three programmatic thrusts: Biodefense characterization, bioforensics, and agricultural security. And these are executed through five research and operations center. An interim capability is currently operational today at Fort Detrick with spoke operations at our national labs.

DHS is also contributing to a governmentwide effort to build U.S. leadership in science and technology. We are reaching out to the academic community to provide students with opportunities to pursue career paths in sectors of science and technology that are vital to our national security. Two examples of this are the Homeland Security Centers of Excellence Program and our Scholars and Fellows Program.

Within the Centers of Excellence Program, the Department plans to establish a network of university-based homeland security centers, each with a different area of focus in research and development. The first center will examine the Nation's resiliency to various acts of terrorism in terms of impact and consequences, using risk-based economic modeling. Seventy universities submitted white papers, and of these, 12 were invited to submit full proposals. We plan to announce the first Center of Excellence in late November.

Also, the first 100 awardees of the Homeland Security Scholars and Fellows Program began their studies this fall. These men and women will study in areas aligned to our mission, such as the life sciences, engineering, computers, information sciences, social sciences, and psychology.

And while the Science and Technology Directorate is ramping up, we have also been very hard at work delivering capability. My statement for the record that I am submitting today includes several examples of the Directorate's current accomplishments as well as capabilities that will be available within the next few months, in the very near term.

Mr. Chairman, Congresswoman Lofgren, and members of the subcommittee, this concludes my prepared statement. I am happy to address any questions you have.

Mr. THORNBERRY. Thank you, Dr. Albright. And let me just compliment you on your written statement. It was certainly more thorough and more direct than a lot that we get up here, and it was very helpful, and I want to compliment you on that.

[The statement of Dr. Albright follows:]

PREPARED STATEMENT OF DR. PENROSE ALBRIGHT

Good afternoon Chairman Thornberry, Congresswoman Lofgren, and Members of the Subcommittee. I am pleased to appear before you today to report on the progress the Science and Technology Directorate of the Department of Homeland Security is making in implementing Title III of the Homeland Security Act of 2002. Dr. Charles McQueary, Under Secretary for Science & Technology, appeared before this Subcommittee on May 21, 2003 and I am pleased to have the opportunity to update you on the status of our efforts to build out the Directorate. In its planning, the S&T Directorate has been guided by the Homeland Security Act, current threat assessments, our understanding of existing capabilities or those that can be anticipated in the near term, and by the priorities outlined in the President's National Strategy for Homeland Security. In short, we are shaping the Directorate to serve as the Department's hub for research and development for exposing and countering chemical, biological, radiological, nuclear, high-explosive and cyber threats against the United States and its people.

Progress in Operations of Key Offices

I am pleased to report that all key offices of the Science & Technology Directorate are operational. Directors with strong credentials have been appointed to each office and we continue to strategically add highly skilled technical, professional and support staff. The offices originally planned are up and running and include: Plans, Programs and Budgets; Research and Development; Homeland Security Advanced Research Projects Agency; and Systems Engineering and Development.

The Science and Technology Directorate is implementing its activities through focused portfolios that address chemical, biological, radiological and nuclear and cyber threats; support the research and development needs of the operational units of the Department; and receive valuable input from private industry and academia as well as national and Federal laboratories.

Office of Plans, Programs and Budgets

The Office of Plans, Programs and Budgets (PPB) is operating under my supervision. I have organized this office into several portfolios, each of which is focused on a particular discipline or activity; taken together, these portfolios span the Directorate's mission space. A key mission for the S&T Directorate is to act as the Department's focal point and advocate for countermeasures to weapons of mass destruction. Thus, there are portfolios that address countermeasures for chemical, biological, radiological, nuclear, cyber, and high-explosives threats. A further key mission for the Directorate is to provide the research, development, test and evaluation for our customers in the other directorates. Thus, there are portfolios focused on borders and transportation security, intelligence analysis and critical infrastructure, and emergency preparedness and response. Finally, there is a portfolio dedicated to developing standards for technologies for homeland security to better aid Federal, State, and local agencies in being smart buyers of homeland security technologies.

Directors are now in place for each of the portfolios and we are continuing to build out our staff. The staff of each portfolio is charged with being expert in their particular area, with understanding the activities and capabilities extant in Federal agencies and across the broad research and development community; and with developing a strategic plan for their particular portfolio, to include near-, mid-, and long-range research and development activities. In addition, I have staff that is charged with understanding the threat from a technical perspective, with inte-

grating the various portfolios into a coherent overall plan, with developing the corresponding budget, and monitoring its financial execution. Finally, I am responsible for executing the Directorate's implementation responsibilities for the SAFETY Act.

Homeland Security Advanced Research Projects Agency

It is our good fortune that Dr. David Bolka joined us last month as director of the Homeland Security Advanced Research Projects Agency, known as HSARPA. Dr. Bolka made significant contributions in advancing technical and scientific projects in his prior work with Lucent Technologies and Bell Laboratories, following a notable Naval career.

HSARPA's Chemical/Biological Technical Office is fully operational. Other offices will address the technical aspects of countering radiological, nuclear, high explosives and cyber threats. Still others will have informational analysis, rapid prototyping/testbeds and conventional R&D as a focus. In addition, an area of special interest for this office will be the role that human psychology plays in terror threats and attacks.

HSARPA is the external research-funding arm of the S&T Directorate. It has at its disposal the full range of contracting vehicles and the authority under the Homeland Security Act to engage businesses, federally funded research centers, universities and other government partners in an effort to gather and develop viable concepts for advanced technologies to protect the homeland.

HSARPA's mission is to identify and develop revolutionary technologies, satisfy DHS customers' operational needs for advanced technology, and quickly produce prototypes that lend themselves to commercial applications. Its customers are State and local first responders and Federal agencies that are allied with homeland security such as the Coast Guard, Secret Service, Citizenship and Immigration, the Federal Emergency Management Agency and others.

HSARPA's first priority is to seed the development of the next generation of chemical/biological sensors and systems to meet anticipated threats under existing conditions. We are interested in a timeline of 6 to 24 months for taking a technology from concept to prototype. HSARPA has engaged the private sector in its first solicitation [HSARPA RA 03–01], seeking detection systems for chemical and biological weapons and associated materials. Interest and response from the private sector has been strong. S&T held a bidders' conference in Washington on September 29 that drew approximately 400 participants and we have received more than 500 white papers as a result. The next step is to select the finalists who will be invited to submit full proposals. We expect to begin contract negotiations in late January.

HSARPA plans to issue a series of solicitations to address radiological, nuclear and high-explosives threats shortly. These and other solicitations will seek to engage our Nation's research and development community, including academia, FFRDC's, non-profits, and industry.

In fiscal year 2004, HSARPA will execute about 40 percent of appropriations for S&T. Nearly 23 percent of the directorate's R&D budget of $874 million will go to biological countermeasures while about 6 percent is for chemical countermeasures. In addition, 10 percent of these funds are dedicated for revolutionary, long-range research for breakthrough technologies and systems, while the rest is dedicated to improving existing technologies that can be developed more quickly.

Office of Research and Development

We are pleased to have Dr. Maureen McCarthy on board as Director of Science and Technology's Office of Research and Development (OR&D). Dr. McCarthy has served as Chief Scientist for the National Nuclear Security Administration and the Department of Energy and was previously DOE's senior representative to the Homeland Security Transition Planning Office. She will lead the office as it strives to provide the nation with an enduring capability in research, development, demonstration, testing and evaluation of technologies to protect the homeland. This office also plans to provide stewardship to the scientific community and to preserve and broaden the leadership of the United States in science and technology.

Activities within OR&D address the resources that can be brought to bear to better secure the homeland through the participation of universities, national laboratories, Federal laboratories and research centers. Directors have been appointed to lead efforts in each of these areas and staff is being added rapidly.

Office of Systems Engineering and Development

John Kubricky joined S&T earlier this month as Director of the Office of Systems Engineering and Development (SE&D). He is tasked with leading the implementation and transition of large-scale or pilot systems to the field through a rapid, efficient and disciplined approach to project management. Mr. Kubricky previously served as Advanced Program Development Manager for Northrop Grumman and

has held senior positions with California Microwave, Westinghouse Defense and with the U.S. Army Ninth Infantry Division.

One of S&T's challenges is to evaluate a wide spectrum of military and commercial technologies so rapid, effective and affordable solutions can be transitioned to Department's customers that include first responders and Federal agencies. In some cases, military technologies could be candidates for commercialization, but rigorous systems engineering processes need to be applied to ensure a successful transition. SE&D's role is to identify and then in a disciplined manner retire risks associated with such technologies to ready them for deployment to the field. In doing so, the office must view each technology through the prism of affordability, performance and supportability—all critical to end-users. SE&D must weigh considerations such as the urgency for a solution, consequences of the threat, safety of the product, lifecycle support and other factors as new products are introduced. Products must be user friendly, have a minimum of false alarms, require little or no training and consistently provide accurate results. SE&D will demonstrate and test solutions before they are released to the field, and will validate that those solutions meet user expectations.

Office of Weapons of Mass Destruction and Office of Incident Management

Under Secretary McQueary created this office to serve as S&T's arm for crisis response. The office assists and provides scientific advice to the Office of the Secretary of Homeland Security in assessing and responding to threats against the homeland. Activities of this office, which is focused on the biological, chemical, radiological, and nuclear threats, revolve around response coordination, providing scientific and technical expertise in developing operational plans and assessment of threats, and continuity of operations.

Collaborative Efforts in Critical Infrastructure Protection

America's critical infrastructure is a web that connects virtually every aspect of modern society. The Department's efforts in this area span 14 sectors and assets that are in need of particular attention. These include agriculture, food, water, public health, information and telecommunications, energy, hazardous materials, and national monuments, among others. A major disruption to any of these sectors will impact others and could have far-reaching implications in terms of quality of life for large numbers of Americans.

Acts of terrorism are not solely about loss of life. Acts can also occur that are aimed at creating widespread panic among our citizens, and disrupting our financial markets and economic well being. The Department's role here is prevention, protection, response and recovery. Adding to the complexity of our job is the fact that much of the nation's critical infrastructure is privately held and not controlled by the Federal government. This underscores the need for strategic collaborations among DHS and other agencies in local, State and Federal government, in academia and the private sector—and I am pleased to say we continue to make strong progress in this area.

S&T supports the Department's Information Analysis and Infrastructure Protection Directorate with research, assessments and guidance in evaluating threats and areas of vulnerability. We provide the technical understanding of the current and evolving threat, such as those posed by biological pathogens and improvised nuclear or radiological weapons. We are providing cutting edge tools to better enable intelligence analysts to organize and query their data, and to better "connect the dots". We are developing decision tools to better understand the vulnerabilities and risks to our infrastructure, so that policy makers can efficiently allocate resources to its protection.

The Department is very aware that our critical cyber infrastructure is an attractive target for our adversaries. DHS has created the National Cyber Security Division under its Information Analysis and Infrastructure Protection Directorate. NCSD operates around the clock to conduct cyberspace analysis, issue alerts and warnings and improve information sharing and stands ready to respond to major incidents and aid in national-level recovery efforts. S&T is, in coordination with IA&IP, creating a robust cybersecurity research and development activity aimed at better understanding our cyber vulnerabilities, and developing tools that make it easier to perform software patches, or detect the insider threat.

National Laboratories, Federally Funded Research Centers and Universities

National Labs

The Science and Technology directorate has created the Homeland Security National Laboratory System. The System, which is comprised of laboratories across the nation, provides the Department with a vigorous internal research component. Di-

rectorate staff members work closely with personnel from each of the national laboratories to promote innovative homeland security solutions. S&T is presently exploring ways for the national laboratories to participate in HSARPA activities.

Homeland Security Institute

The Homeland Security Act requires that DHS establish a federally funded research and development center known as the Homeland Security Institute to assist the Office of the Secretary and the S&T Directorate in addressing important homeland security issues that require scientific, technical and analytical expertise. To start the process, DHS, working with the Army's U.S. Medical Research Acquisition Agency Activity (USAMRAA) issued an early notice on September 10 seeking expressions of interest and qualifications, which are due today, October 30. The results of this effort will assist DHS and USAMRAA in developing a major solicitation for this activity. Plans call for the staffing of the office to begin November 1 and the formal solicitation to be issued in December.

Among other functions, the Homeland Security Institute may be tasked with designing metrics to evaluate the effectiveness of homeland security programs throughout the Federal government including the national laboratories.

Universities

Through the Office of Research and Development, DHS is contributing to a government-wide effort to build U.S. leadership in science and technology. The office is reaching out to the academic community in an effort to provide students with opportunities to pursue career paths in sectors of science and technology that are vital to our national security. Two examples of this are the Homeland Security Centers of Excellence program and our Scholars and Fellows program.

With the Centers of Excellence program, the Department plans to establish a network of university-based Homeland Security centers, each with a different area of focus in research and development. The first Center will examine the nation's resiliency to various acts of terrorism, in terms of impact and consequences, using risk-based economic modeling. The Department's call for white papers regarding the initial Center drew over 70 responses. S&T narrowed the field to 12 universities that submitted full proposals earlier this month and plan to announce the first Center of Excellence in late November.

The Homeland Security Scholars and Fellows Program provide scholarships for undergraduate and graduate students pursuing degrees in areas that are already aligned with our mission. The first 100 awardees of this program began their studies this fall. These men and women will study in areas such as life sciences, engineering, computers, information sciences, mathematics, physical sciences, social sciences and psychology.

National Biodefense Analysis and Countermeasure Center

The National Biodefense Analysis and Countermeasure Center (NBACC), based at Fort Detrick in Maryland, is the hub within homeland security for research and operational capabilities to anticipate, prevent, respond to, and recover from current and next-generation biological threats to the American people and our agricultural system. NBACC is dedicated to protecting human health and agriculture by advancing the scientific community's knowledge of potential bioterrorism. NBACC aims to achieve efficient interagency and private sector cooperation with a structure that integrates facilities and technical expertise in biodefense and involves Plum Island Animal Disease Center, national and DHS laboratories, universities, the private sector and other government agencies. Biodefense characterization, bioforensics and agricultural security are the key programmatic thrusts of NBACC that are executed through these five research and operations centers: Biothreat Assessment Support Center; Biodefense Knowledge Center; Bioforensics Analysis Center; Bio–Countermeasures Testing and Evaluation Center; and the Plum Island Animal Disease Center.

Homeland Security Science and Technology Advisory Committee

The Homeland Security Act required the S&T Directorate to put together a committee of 20 prominent individuals with expertise spanning the Directorate's activities. They are to act, in essence, as our board of directors, advising the Under Secretary on the best ways S&T can deliver to the American people the technology and cutting edge capabilities that are a fundamental strength in the war on terrorism. We have decided on the people we would like to serve on that Committee, and are contacting them now. I expect the Committee to meet for the first time early in December.

Accomplishments

While, the Science and Technology Directorate has organized itself, is rapidly staffing up, it also has been at work delivering capability. I would like to mention

some examples of current accomplishments as well as capabilities that will be available within the next few months.

Biological and Chemical Defense Programs:

- The Biowatch program has been established and deployed to numerous cities across the nation. The program, developed, funded, and managed by the S&T Directorate, is executed in cooperation with EPA and CDC. It employs environmental sampling devices to quickly detect terrorist agents, such as anthrax, in time to distribute life-saving pharmaceuticals to affected citizens. The Science and Technology directorate is now focusing its efforts on piloting the next generation of environmental samplers which will reduce the amount of labor required and response time needed for devices while keeping the detection probability high and false alarm rates low.
- The S&T Directorate and the Washington Metropolitan Area Transit Authority (WMATA), recently completed PROTECT (Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism). PROTECT, which is an operational chemical agent detection and response capability program, is deployed in more than six stations and operated by the WMATA. Upon completion, the system will be totally owned and operated by WMATA and expanded to approximately 20 stations. The information gleaned from PROTECT will have direct applications to similar facility protection and response efforts across the nation.
- In June 2003, the Science and Technology directorate, in coordination with the Department of Defense's Defense Threat Reduction Agency, Department of Energy, and University of Oklahoma sponsored a month-long atmospheric dispersion study in Oklahoma City, OK. Nearly 150 scientists, engineers, and student assistants were dedicated to this study, which tracked the air movement of safe, non-toxic tracer gases in and around city buildings. The resulting data is being used to enhance and develop urban specific computer models that will allow emergency management, law enforcement and other personnel to train for and respond to potential chemical, biological, and radiological terrorist attacks.

Interoperability of Communications:

- The Department is taking steps to boost the ability of 44,000 local, tribal and State entities and 100 federal agencies engaged in public safety to communicate effectively with one another, particularly during an emergency. SAFECOM is a Federal umbrella program under S&T that is dedicated to improving public safety response through enhanced interoperable wireless communications. The goal is to enable public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice or data with one another on demand and in real time. SAFECOM is providing seed money for the Department of Justice's Integrated Wireless Network program which will create interoperability among local, State and Federal public safety agencies in 25 cities. In addition, technical guidance for interoperable communications that was developed under SAFECOM will be included in this year's Office of Domestic Preparedness grants.

Information Analysis and Infrastructure Protection Programs:

- Analysts from S&T built and delivered a prototype system to IAIP to perform Graphical Information System (GIS) based computer assisted threat and vulnerability mapping of the oil and gas infrastructure in the American Southwest. S&T is also in the process of delivering to IAIP cutting edge visualization, data searching, data correlation, and all-source analytic aids to provide IAIP advanced analytic capabilities integrated with vulnerability information.
- The Nuclear Assessment Program is engaged in ongoing assessments and analysis of communicated nuclear threats and claims of illicit trafficking in nuclear materials. This program also inaugurated a new capability to rapidly analyze gamma and neutron spectroscopy in support of Customs and Border Patrol officers to quickly resolve radiation anomalies at the borders. This capability is in the process of being expanded, through the National Biodefense Analysis and Countermeasures Center, to the biological domain.

Border and Transportation Security Programs:

- The Science and Technology directorate has initiated the Border Safe Integrated Feasibility Experiment. This experiment creates an infrastructure in the Southwest United States for data sharing between the Department's Border and Transportation Security directorate and local and State law enforcement officials. The resulting system will identify individuals who have already entered our country, either legally or not, and who engage in hostile behavior after

crossing the border. The system will particularly focus on individuals who attempt to change their identity or borrow someone else's identity.

• S&T has deployed to sites in the New York metropolitan area (tunnels, bridges, ports and airports) various nuclear radiation technologies. This demonstration effort involves transition of state of the art, new detection technologies available at the National Labs to the field, the development of operational concepts and technical reach back procedures, and on-site alarm resolution. It will serve as a model for deployment of these technologies to the interior of the Nation, around major urban centers, and at ports and airports.

Portable Air Defense Systems:

• The Department of Homeland Security has developed and submitted to Congress a program plan for countermeasures against the shoulder-fired missile threat to commercial aircraft, known as MAN–Portable Air Defense Systems (MANPADS). Based on this report, the Science and Technology Directorate established a program office to oversee the Department's MANPADS efforts. These actions are aimed at leveraging existing military research and development programs, and re-engineering those capabilities so that they are consistent with airport operations and commercial air carrier maintenance, support, and logistics schemes.

• In September, S&T released a solicitation announcing a program to address the potential threat posed by MANPADS. The solicitation is the first step in the Department's two-phase systems development and demonstration program for anti-missile devices for commercial aircraft. Phase I will provide an analysis of the economic, manufacturing and maintenance issues needed to support a system that will be effective in the commercial aviation environment. Phase II will include development of prototypes using existing technology which will be subjected to a rigorous test and evaluation process. The Department held an Industry Day in Washington, DC on October 15 to brief contractors about the program. White papers responding to the counter-MANPADS program solicitation are currently being reviewed. Respondents receiving favorable reviews will be encouraged to submit full proposals.

Maritime Security:

• The Science and Technology directorate's Homeland Security Advanced Research Projects Agency (HSARPA) has joined with the U.S. Coast Guard to build a prototype integrated maritime surveillance facility covering Port Everglades, Miami and Key West. The $3.7 million, 24-month program will integrate existing facilities and upgrade equipment to detect, track, and identify vessel traffic around ports, in the near-shore zones around ports, and over the horizon. This evolutionary testing will provide an immediate coastal surveillance capability in a high priority area; offer the U.S. Coast Guard and other Departmental organizations the means to develop operational concepts; and implement and test interoperability among Homeland Security and Department of Defense systems and networks.

SAFETY Act:

• On October 10, 2003, Secretary Ridge signed an interim final rule implementing the Support Anti–Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002. The SAFETY Act is designed to encourage the development and rapid deployment of life-saving, anti-terrorism technologies by providing manufacturers and sellers with limited liability risks. The Department is now accepting applications for designation under the Act.

• In October, the Science and Technology directorate led a series of nation-wide seminars (Dallas, Los Angeles, Atlanta, Chicago and Washington) to introduce the process to implement the SAFETY Act. The seminars provided general information about the Act, introduced the pre-application process, and provided a forum for questions about the Department's implementation processes.

Standards:

• Staff members of the Science and Technology directorate are working with the emergency responder community, and other federal partners such as NIST, to develop standards. Initial guidelines for radiation detection technology have already been made available, with formal standards nearing completion. Standards are also under development for detectors of biological hazards. Guidelines have been published for interoperable communications gear.

• The Science and Technology directorate is working with other Federal partners to develop a set of standards for cleanup after a biological or radiation incident. By providing states and localities with cleanup guidelines, potential hazardous impacts can be significantly decreased.

Mr. Chairman, Congresswoman Lofgren and Members of the Subcommittee, this concludes my prepared statement. I am happy to address any questions you may have.

Mr. THORNBERRY. I would be happy to yield my time to the chairman of the full committee, if he would like to ask questions at this point.

Mr. COX. Thank you, Mr. Chairman.

Welcome again, Dr. Albright. Two of the things in your prepared testimony prompt me to ask for additional detail. One is the experiment that you have initiated for Border and Transportation Security. It is described in your written testimony briefly as the creation of an infrastructure in the Southwest for data-sharing between DHS and Border and Transportation Security Directorate on one hand, and State and local law enforcement on the other hand. The aim is to identify people who are doing bad things once they cross the border and perhaps in the process also swapping identities.

How is this going to work? How is it working already?

Mr. ALBRIGHT. Well, it is set up in, I believe, a couple locations. I believe it is set up in southern Arizona, along the Arizona border, and it is also set up in southern California. And in essence, you have described the program to a T. What it is is that as people who—the State and local people who—the State and local people will tell our border people who they have a particular interest in. And as these people cross—.

Mr. COX. How do they do that? How do they tell DHS?

Mr. ALBRIGHT. Sir, I would have to get back to you on the actual details of that, but my understanding is they have basically created a watch list of individuals and names that they are interested in seeing cross the border. But the actual mechanical details of that I would have to get back to you on.

Mr. COX. And the brief description that you provided states that you are going to identify individuals who have already entered the country, either legally or not. Is there any coordination between the Border and Transportation Security Directorate and immigration?

Mr. ALBRIGHT. Sir, yes, I believe there is. We have been working—as we have been implementing this program, we have been working closely with the senior staff.

Mr. COX. What I mean to ask is in addition to inputs from State and local law enforcement, are we attempting to match up information that we have already collected within this Directorate and within DHS, for example, from US-VISIT or from anything else that we are running?

Mr. ALBRIGHT. Well, it is my understanding that the answer in general is, yes; that basically we are matching up information. To the degree that we have those databases integrated today, that information is being matched up. Of course, US-VISIT itself isn't up and running yet, so that hasn't been happening yet.

Mr. COX. But neither is this program. It is an experiment.

Mr. ALBRIGHT. No. Right now there are no experiments either from US-VISIT. There is obviously—in southern California, for example, there is a sentry program, but that only applies to preapproved individuals when they cross the border, and those tend to be fairly low-threat people.

Mr. COX. I wanted to ask you also about your efforts to focus on communications interoperability. SAFECOM is focused on both voice and data. You have also apparently been connected somehow fundingwise to DOJ and the 25 cities that they are working in. What exactly are we doing, apart from that DOJ project, in DHS on interoperability with SAFECOM?

Mr. ALBRIGHT. Okay. As you know, SAFECOM is a DHS-managed activity, but it is part of the—it is a Presidential management initiative that actually relies on contributions from across the Federal sector. So you are quite right, DOJ is a player in this, DOD is a player in this, although DHS is managing it and does do the bulk of the funding, I might add.

Sort of the 25 cities that are within the public wireless network program within SAFECOM are the key testbeds for interoperability. However, we are also conducting additional activities. For example, what SAFECOM is doing is sort of its key role is developing technical standards for interoperability. And what we have recently done, and this is the first time this has happened, is the guidance associated with those standards has been included in the suite of grants that have been issued by ODP, by FEMA, and also by the COTS program. So what we are starting to see now is a uniform set of technical standards that are being issued across all the grants programs that DHS is involved with.

Mr. COX. In addition to a standard setting, is there any other aspect of the program?

Mr. ALBRIGHT. There is certainly a lot of issues. Clearly, there is—as you said, there are testbeds occurring in multiple cities that we are leveraging. There are a lot of issues, as you are, I am sure, aware of, especially with spectrum management that we are concerned about. There is technology issues. But those are the key—the two activities which are the testbeds and the standard setting are the key activities within the program.

Mr. COX. The last thing I want to ask you about is IP and our focus on, for example, the grid and recent demonstration of the problems with the New York blackout. How has the S&T Directorate collaborated with IA&IP to mitigate this vulnerability? How have you leveraged industry, if you have, to be a key partner in providing tools? What other tools are you bringing to bear?

Mr. ALBRIGHT. Well, there is a couple of things we have been doing with respect to the electrical blackout, the specifics of that. The first is—is, yes, in fact, we are—we have been engaging in industry to understand better these sorts of tools and predictive tools that may be available to—as you say, to help us do a better job of modeling the infrastructure and understanding where some of the key vulnerabilities are under the sets of circumstances that we saw occur in that particular blackout.

We are also working closely with Bob Viskowsky and his people in the analysis of the data that has come out, that is coming out of this blackout. I mean, the blackout was a—it was obviously not a terrorism event; but from the perspective of the Department of Homeland Security, it is a wonderful opportunity to learn better some of the issues that are associated with, for example, interdependencies among infrastructures that so far have been primarily the subject of speculation, or, frankly, people sitting around

a room kind of making lists up. This is an opportunity for us to actually put some facts on the table and understand that if an electrical power system goes out in Cincinnati, what effect it has, say, in Alabama, you know, on some industry because the supply chain got broken.

So those kinds of analytical—that kind of analytical support is something we are providing directly to—as part of our systems engineering responsibilities, within the Department, to the IA&IP folks.

Mr. COX. I thank you very much.

And I thank you, Mr. Chairman, on that last point. You know, whether it is transportation or food supplies or energy reactors, the threat that links all of these together is the our cybernetwork; and obviously focusing on the grid and on blackouts is vitally important and a big responsibility of this subcommittee.

Mr. THORNBERRY. I thank the Chairman.

Ms. LOFGREN.

Ms. LOFGREN. Thank you, Mr. Chairman.

I am wondering. We are about 6 months into this, and we are basically—this part of the Department was being built from scratch, so I am wondering if you can tell me how many full-time employees the Directorate has on staff, and then how many additional people you have in detailees and contractors, and then what the final level will likely be.

Mr. ALBRIGHT. Okay. I will try to give you an answer that was good as of this morning.

Ms. LOFGREN. That would be fine.

Mr. ALBRIGHT. Because it changes rapidly.

I believe that the number of full-time employees that we have on board in the S&T Directorate—within the headquarters activity, I think, is 110. It is roughly 110. We have on top of that another 30 or 40 contractors who are called SETA support contractors or detailees from other agencies. For example, we have a detailee from NIST who supports us. Actually we have a couple from NIST. So the net result is about 150, 160 people.

Our full-time staffing level in terms of government employees, we expect to be fully staffed in the headquarters activity around 180 or so, with another additional 50 or 60 contractors or detailees. We have got three AAAS fellows, you know, people like that on board.

Ms. LOFGREN. Along those lines, I have had some people express concern, and I don't know if it is—whether we should be concerned, so it is a question, about the depth or breadth of the science experience in the leadership. I believe you are a physicist, and Dr. McQueary is an engineer, and Dr. Bolka is a physicist, and Dr. McCarthy is a nuclear chemist, all of which, I mean, is pretty impressive. But there isn't anyone from the biology part of our science world. And is that something that we are going to address as we move forward? Do you think it needs to be addressed?

Mr. ALBRIGHT. We have—in terms of the senior leadership, you are quite right. But I have to tell you, I don't actually do a lot of physics in my job anymore. I guess I could have been glib and say that physicists think all science is a branch of physics.

Ms. LOFGREN. I have heard that.

Mr. ALBRIGHT. Right. But actually we have several people with biological training on board. I have a portfolio that is the bio—and I have got the chemical threat also in there as well, mainly because that is how I am staffed up right now. And I have got a number of—I have got a veterinary—I have got people who do veterinary research in that group. I have research people with biological degrees, immunologists, virologists. So we have access to that kind of talent where we need to have it.

Ms. LOFGREN. And you don't feel that it is a problem in terms of prioritizing the issues?

Mr. ALBRIGHT. Not at all.

Ms. LOFGREN. All right.

I am interested in the—I call it "SARPA," not HSARPA, because DARPA is easy, it flows from the tongue; "SARPA" flows from the tongue.

Mr. COX. If the gentlelady would yield. The H should be silent; don't you think?

Ms. LOFGREN. Yeah. It is "SARPA." And that way we will live and flourish and grow.

As I understand it, HSARPA is now focused on more near-term, immediate type of needs. But DARPA really has been—that has been so successful over the years, and we have benefitted so much as a Nation from DARPA, really has a longer-range agenda. Do you see HSARPA morphing into that DARPA model down the road? And, if so, when? And, if not, how are we going to get those long-range functions accomplished?

Mr. ALBRIGHT. That is an excellent question, and I will try to call it "SARPA" from here on out. It is about the third thing we have tried, so we will try that.

DARPA—first, let me say that HSARPA is always going to have a long-range research component, you know, a piece of it that is always looking at sort of crazy ideas, you know, things that, you know, no one else might be thinking about. And I certainly see that growing. But I think the name HSARPA is an unfortunate one for the Department of Homeland Security because it does bring to mind DARPA, and there are some very distinct differences between the environment which DARPA operates in and the environment that we operate in.

If you look at DARPA, DARPA exists in an environment where there are already significant service acquisition activities within each of the military services. So, for example, for a lot of the directed research that you get in the military and the Pentagon, that directed research—if I needed a new surface air-to-air missile, I tend not to go to DARPA for that, I tend to go to Wright-Patterson for that, for example. If I need a new submarine, I don't go to DARPA for that typically. And the reason for that, of course, is you have these very robust evolutionary capabilities within the respective services as they fulfill their Title X responsibilities.

So DARPA is in a sense a very needed but additional piece onto that infrastructure that allows the Pentagon to often—and focus solely on those kinds of things that don't pop up through the evolutionary acquisition chain.

In the Homeland Security Department, in S&T, HSARPA is it. That is our acquisition chain. And so to the degree which we have

to—so it becomes—what you are really saying is that there is a management challenge that we are always going to have, which is to make sure that we always reserve funds in our budget to assure that HSARPA does have the wherewithal to conduct that DARPA-like activity within its overall responsibilities. And the way we have chosen to do that is we have created a portfolio and a budget line that we call emerging threats, and this year in 2004 I believe it is around $25 million, and that money is there for exactly that purpose, to allow HSARPA, without any direction from anybody else, from any of the other portfolios, to basically have the Director go off and try out those things that we didn't think are good ideas, but he thinks are good ideas and ought to explore. And that is what that is all about.

Mr. ALBRIGHT. And that is what that is all about.

Ms. LOFGREN. I have only a moment left on my time, but we have asked a variety of witnesses, including the Secretary himself, whether we can provide technical assistance to the immigration function so that they can deploy technology; and I am so frustrated with this. I mean, in my other job as a member of the Immigration Subcommittee in Judiciary, we have been beating them up for years to deploy technology, and I do not see anything happening.

Have you been able to assist them? Is that on your to-do list? Could you give us a report on it?

Mr. ALBRIGHT. That is very much on my to-do list, and the Secretary has put it on our to-do list.

A lot of the activities, of course, are focused with the US-VISIT program that Mr. Cox was referring to earlier. There is a statutory requirement to deploy machine-readable documents at the border, so we have been looking closely with the US-VISIT program and with the BTS people to help them sort through what needs to be done there.

As I am sure you are well aware, the NIST has a very large activity associated mainly with setting standards for fingerprints. That is sort of what they tend to focus on, but on other areas, in particular in the areas associated with fusing different kinds of biometrics, we have been very actively engaged on that. In fact, we have a research program designed to explore those issues; we are working jointly with NIST to create a database that allows us to perform that work, and so, yes, we are pushing forward on that.

Ms. LOFGREN. Just one final remark: That sounds good, but they are still creating paper files in Immigration.

Mr. ALBRIGHT. I know, I know, and that is a separate issue entirely about whether or not—you are absolutely right. They create paper files and those paper files sit in archives in Pennsylvania for 100 years.

That also is being worked, not so much by us, but by the people in Immigration, who do immigration, who are pushing for a modernization program along those lines.

Mr. THORNBERRY. I thank the gentlelady for some excellent questions.

The vice chairman of the subcommittee, Mr. Sessions.

Mr. SESSIONS. Thank you, Mr. Chairman, and thank you, Dr. Albright, for being with us today. I will be very quick in my question to you so that it will allow you time before we go vote.

I notice on page 7 of your report to us, Accomplishments, the Biowatch program. I would like to have you discuss that, but my tee-up is: You talk about going all around the country, being prepared for things that are ahead—SARS, anthrax, these sorts of things. Can you please tell me about those successes? And how prepared are we, how much better prepared are we than what we were for the things that we have been through; and in your opinion, what do we have to look forward to and what can this committee do—subcommittee and committee do to help you further?

Mr. ALBRIGHT. Thank you.

Let me first talk about Biowatch.

As you know, Biowatch is an environmental sampling program that we have in place in 31 cities across the country, and what we have done is deploy environmental samplers that suck air continuously and the results from that sampling are then taken to the CDC's Laboratory Response network labs for analysis; and this is done in full coordination with CDC and EPA, and the idea basically is to provide sufficient warning of, for example, an aerosolized anthrax attack in a time sufficient for us to be able to deploy the stockpile and to treat the people who have been affected.

We also have significantly improved our plume modeling capabilities at the NARAC facility out at Lawrence Livermore National Laboratory, which allows us to understand where the contaminant plume has gone, to help us better focus our efforts; and we are working closely with HHS and CDC, not just on the Biowatch program, but also in the development of medical surveillance capabilities to also help warn us if an event has occurred and to help HHS and the National Institute for Infectious Diseases—Allergies and Infectious Diseases to help prioritize their program.

Almost certainly the first procurement out of the bioshield program, should the bill be signed, would be the RPA vaccine for anthrax, which, if deployed and if we are able—certainly it would be deployed to first responders and may, if we can get it right, be deployed nationally. That will take anthrax off the table entirely.

Mr. SESSIONS [Presiding.] I thank the gentleman for his response.

Chairman Thornberry has left to go vote. We are going to continue on with this hearing for your being so gracious to stick with us when we were in trouble; and I will now yield the time to Mr. ndrews from New Jersey.

Mr. ANDREWS. Thank you, Doctor, for your excellent testimony.

On page 2, you talk about the directorate or the portfolio dedicated to developing standards for technology for homeland security, and Federal and State and local agencies and being smart buyers of homeland security technologies. I think this is a crucial issue. I think we were wise in decentralizing responsibilities for homeland security to those who know their turf best. But that strategy will work only if people do not buy junk, and I am very concerned that we have standards in place so that local buyers are given a lot of guidance into what they ought to buy and not buy.

The specific question I have for you is whether you anticipate the standards that your group will develop being incorporated into grant contracts with local grantees, or will they simply be suggestions?

Mr. ALBRIGHT. We haven't gotten that far yet. So far, the thinking has been that it would be in the grant guidance, so we would tell people that this is something they certainly ought to do. I do not know if we will require it or not; and to be honest with you, I think it will matter a lot on what the equipment is. There is certainly a kind of equipment where, I would imagine, we might be very—pretty insistent on that, because when an alarm goes off, we are the ones who get called.

Mr. ANDREWS. Right.

Mr. ALBRIGHT. On the other hand, for other sorts of things, we may just leave it up to the guidance.

Mr. ANDREWS. I would strongly urge you to consider incorporating standards into the actual contract documents.

You know, port authorities and airport authorities are creatures of local politics, and one of the benefits of that is, they are very responsive to their local community, but one of the risks is that a technology is going to be purchased because someone's brother-in-law is selling it or someone's contributor is developing it. It has been known to happen in American politics.

I think it would be, at best, a waste of taxpayers' money and, at worst, a disaster if a technology that purports to protect against a biological or chemical attack fails because it doesn't meet standards. I think it is imperative that an operation like yours, that has the credibility and the scientific expertise, develop these standards and require they be applied in these contracts.

The second point that I would make is about the role of the private sector, which I know you acknowledged in your written statement. You have a difficult balancing act, but I trust that you will be able to follow it; and that balancing act is, I think you need to reach out to the very best in the private, university and nonprofit sectors but do so in a way that doesn't prejudice your standard of development that benefits their particular proprietary product.

It is an easy thing to say, but a hard thing to do.

Have we given you the legal tools necessary for you to accomplish that mission, or do you need other legal tools?

Mr. ALBRIGHT. Right now, I think we are in great shape. The point you brought up is something we do talk about quite a bit, and that is—as you know, when you do consensus standards, you have to be very, very mindful of the fact that someone might be trying to, you know, wax the alleys. And so what we do is—we are dealing with some pretty experienced people out at NIST, and they understand the issues—and what we do is we certainly—it is very important that we get industry to buy into what we do, but at the end of the day, the standard is issued by us.

Mr. ANDREWS. The reason I feel so passionately about the inclusion of the standards as a condition of the contract is, since September 11, I could do nothing but sit in my office and meet with people who purport to have homeland security technologies that will save the world.

Now, many of them are very well-intentioned, eager people. Some of them are wackos, frankly, and I do not really have the technological expertise to distinguish between the two, and I do not think a lot of local decision-makers do either. I respect them and I respect their local prerogative, but I think it is very important that

we not send Federal taxpayers' money to local people that would buy—in good faith, buy products and technologies that would not work.

I thank you for your testimony.

Mr. SESSIONS. I thank the gentleman.

I would advise us, at this time, that despite what I previously said, we have now been given the information that there are a series of votes, at least one additional vote; and so, as a result of that, we would ask if you could please stand by.

Mr. ALBRIGHT. Sure, no problem.

Mr. SESSIONS. Dr. Albright, it is our intent to come back in just a few minutes after the vote, so at this time, the subcommittee will be in recess.

[Recess.]

Mr. THORNBERRY. [Presiding.] We sure appreciate your flexibility. It is a little difficult for us to even figure out what is happening next, and I am not sure it is going to improve tremendously, but in the meantime, we will do the best we can.

I yield to the distinguished gentleman from North Carolina at this point.

Mr. ETHERIDGE. Mr. Chairman, and to our witness, Dr. Albright I thank Dr. Albright for your flexibility today.

We find ourselves a lot like you, where you talked earlier today—and let me return to that—as relates to HSARPA's mission to identify developing revolutionary technologies to satisfy the operational needs.

I guess all of us have some major research capacity in our districts, but we have an awful lot in North Carolina as relates to the Research Triangle and our world class universities; they are very interested in the work that HSARPA is going to be doing. These universities, as you well know, have a long history of experience with rapid prototyping of new technologies, and that is what we are talking about and what you had talked about, and it is in your testimony.

My question is: What is the director's intent for the $45 million of additional research and development funds appropriated for rapid prototyping?

And let me get my second one in so maybe you can combine your answers: How is the director planning to select products for rapid prototyping? And how will you go about producing and testing the prototyping?

Mr. ALBRIGHT. Okay.

Okay. First, obviously, by rapid prototyping, what we mean is technologies that are commercial off-the-shelf or government off-the-shelf technologies that may have been used for some purpose or another mode and maybe need to be commercialized and perhaps adapted to homeland security purposes; and the way we have chosen to do that, up to now, has been to basically go to our user communities—EP&R, B&TS, IAIP—as well as within our own equities with S&T.

As you know, we have a mission to be service advocates for the chem-bio-rad-nuke weapons of mass destruction issues. So what we do is, we ask ourselves what are the kinds of things we can have that would change the way we do business right now; and what we

do is, we put together a broad agency announcement. It is very similar to a small business, innovative research kind of booklet, if you are familiar with those sorts of things. We publish that and we ask people to respond, and we try to have a very friendly way of doing that, where people will respond in stages.

They send us maybe a chart with just a single sheet of paper and we encourage maybe some of those to respond with a white paper and maybe some of those to respond with a proposal; and this is all aimed at making sure that small businesses in particular do not have to make an extraordinary investment in running a full proposal before they get things in to us, and then we evaluate those for our immediate needs and fund them. That is how we do it.

The advantage to doing it that way, of course, is that you have the buy-in from the very beginning with the user community, the people who actually are going to deploy this. We are asking them specifically, If we make this for you, will you deploy it? And if the answer comes back, no, then we tend to be not too interested in doing anything with it.

So that is, in essence, the philosophy.

With the extra $45 million that was appropriated to us, clearly we can do more of that. We did that with the $30 million solicitation just last—just a few months ago. There are some additional, perhaps more focused solicitations that we could do in particular areas, and that is one of the options we are considering now.

In some of the IAIP areas, in some of the EP&R areas in particular—and we haven't really settled down yet as to how we are going to spend that, and we are going to have a broad-based solicitation like we did before, but have more money in it, but we are going to do that for part of the money and then have more focused solicitations.

The other thing we need to do, and we need to use a portion of that money for that, is to provide the rest of the clearinghouse function that you all asked for in Section 313 of the act; and that is to take some of that rapid prototyping capability and some of that commercial and off-the-shelf governmental technology and put it into a database that State and local people can address and look at and get some insights as to whether or not this is something they ought to be thinking about buying.

Mr. ETHERIDGE. Thank you.

Let me move to the agroterrorism piece, because as you know, most of that has been delegated to the Department of Agriculture, but as you know, the DHS Science and Technology Directorate is supposed to address countermeasures for chemical, biological, radiological, nuclear, and cyber high-explosive threats.

Can you describe the research efforts that relate to agroterrorism on the agriculture side; and secondly, is DHS coordinating with the Department of Agriculture in this area; and finally, I hope you will share with us what DHS is doing to address the security problem that GAO has just released, as relates to Plum Island Animal Disease Center.

It is important to a lot of States, but it is particularly important to this country with Plum Island. And you might want to talk about what Plum Island is, so I will not use all my time on that.

Mr. ALBRIGHT. Okay. Let me first talk about—let me first talk about our agricultural bioterrorism work.

Most of our focus is on the catastrophic terrorism end of this and so, frankly, our focus has been on foot and mouth disease. That is the one that, if that gets out, that is—all the models pretty much show the same thing. There is no disease more infectious than foot and mouth disease, and so what we have been focused on has been to look at what USDA has been doing; and I will tell you, we are looking very closely with them.

I spend a lot of time with their leadership and my staff spends quite a bit of time with them, as well, crafting out a joint strategy that addresses—their main concerns tend to be focused on natural outbreaks, and natural outbreaks have a certain set of protocols and issues attached to them that are fairly well understood, and they have led to a certain kind of infrastructure. For example, right now, if we have a foot and mouth disease sample, it always gets shipped back up to Plum Island for analysis because they are able to constrain the outbreak in the meantime, the local veterinary people can do that.

If we had a delivered introduction, it is not at all clear you can do that, so that leads you to think about the development of new diagnostic tools that we can, in fact, put out into the field in the State veterinary facilities, so that they can actually perform a more robust identification of the disease in situ. So that is certainly an example of the sorts of things we are talking about.

We obviously are also involved heavily with them on modeling and simulation activities, but basically what we are in the process of now—and this is actually, this is a report to Congress that is requested in early January—is crafting a joint strategy that allows them to continue to do the things they have been doing for a very long time and then allows us to address the infrastructure issues associated with terrorism attacks.

With regard to Plum Island, well, as you know, we took it over, I believe it was June 1; and what we immediately did was, we did a site survey as you would when you are buying a house. For example, you go do a look, and we determined that the smart thing to do at that point was to do a 60-day study across the board of all the various issues associated with Plum. So we looked at infrastructure, we looked at compliance with the bioterrorism rules and regulations, we looked at security quite a bit, and we published that 60-day study, we completed it, and we are now undertaking remedial action on some of the top issues.

The GAO report—we actually feel the GAO report was fairly accurate; I mean, it, I think, reflects the state of affairs when we took the facility over; and all I can tell you is that we are working very, very hard to bring a cultural change to the place—and I should tell you, it has been fairly successful so far, not completely, but fairly successful so far—to get people to think about the fact that, yeah, there is a bioterrorism act out there, and they do have to be cleared to handle some of the pathogens and we do have to be solicitous of what the rules and regulations are.

We have also changed the site contractor as well, so we are doing the best we can to get that site on-line.

Mr. ETHERIDGE. Thank you, Dr. Albright.

Mr. Chairman, as you well know, that Plum Island is an important place in this country, one of the few places that we can do the testing that needs to be done in this country, and it is critical that that security be there.

Let me say, even though my time has expired, that we did a simulation in North Carolina, with the help of people here in Washington and the State folks, on hoof and mouth disease; and I can tell you, without exaggeration, it was frightening what it could do in this country.

Thank you, Mr. Chairman. I yield back.

Mr. THORNBERRY. I thank the gentleman and I have participated in such exercises as well.

Let me kind of take, I guess, a next step from Mr. Etheridge's questions, Dr. Albright; I want to ask about coordination of R&D—first question, within the Department, and secondly, among departments. It is my understanding that there are various elements of the Department of Homeland Security that continue to have their own R&D budgets. TSA, for example, the Coast Guard, possibly FEMA, IP, perhaps.

I would be interested to know what other elements of the Department have an R&D budget, and how it is that you or somebody fits all of those pieces together to make sure that we are not duplicating and we are doing the right thing.

Mr. ALBRIGHT. Okay. First, let me make a distinction between having an R&D budget and having R&D activities.

There are a number of agencies with the Department that historically conducted research and development activities out of operations, of support funds, okay; so they are not identifiably R&D funds. And just the short answer to your question is, the agencies within DHS that do that—other than ourselves, of course—are, let's see, TSA, DCP, former Customs people, INS has a very small 400K budget, Coast Guard, security services, and IAIP picked up several activities as well when they were put together; and I believe that is the list, without having it in front of me.

When we were planning the transition to the new department last year, the decision was made at the time that we would leave well enough alone in 2003, we would exert an oversight function—"we" being S&T—in 2004, and the idea would be to integrate these capabilities within S&T in the 2005 time frame, and that was just a matter of what we thought was the logical thing, the expedient thing to do at the time.

Secretary Ridge made it clear last summer that he expects that integration to occur; and as you are probably aware, in our appropriations language for the 2004 budget, there is a requirement that we present a combined R&D budget in 2005; and, in fact, we are due a report to Congress this December 15 on how we are going to actually do that. So there has been for some time an activity within our CFO shop that has been looking at identifying the R&D activities and then working toward some sort of integration.

Now, there are a couple of caveats I should give you. One, of course, is the Coast Guard, which does have an R&D activity. The Homeland Security Act keeps them as an independent entity, so they would remain that way unless, of course, they specifically de-

cided that they wanted to divest themselves of R&D activity and they got statutory relief.

There are other issues, for example, the U.S. secret Service. There are certain R&D activities they do that it is not clear that it would make a lot of sense to actually, literally bring into our budget process. For example, the R&D on the President's limousine may not make sense.

And so we are looking at all of that, so at least in terms of the internal piece of this, we expect to have a combined budget and have everything integrated within S&T, to the degree it makes sense to do so, certainly within the next couple of months.

We certainly, as I said, have to have that report to the Congress in the next couple of months.

Mr. THORNBERRY. Let me ask—and I understand, for example, the example you gave of the Secret Service. They have some unique responsibilities doing their own research in those areas, and it makes sense, but for example—and that may well be true with Coast Guard, too. But what is then the communication between the S&T Directorate and the Coast Guard for things that may well be overlapping, for example, related to port security in some way.

Mr. ALBRIGHT. Okay. What I have in—what I have done within—as we created the S&T Directorate, as I mentioned in the beginning, we have these portfolios; and several of these portfolios are focused on our CBRN missions, so I have, for example, someone who does bio-chem—I mentioned that earlier—we have someone who does rad-nuke, and there were experts in that area.

In order to make sure that we had this kind of coordination, we also created portfolios at the beginning of the—when the Department stood up for EP&R, for IA, for IP, and for BTS, and the person in those portfolios, their job—and we also have one for the Coast Guard and one for the Secret Service—their job is to make sure that we understand the R&D needs associated with those particular entities. It is their job to work with the user community to make sure that we know what is going on over there, and that they know what is going on over here, and frankly, so that we can help them out. Because, as you know, for a lot of these agencies, their R&D efforts are sitting in an environment where they are constantly competing for operations and support dollars, and, therefore, they have never had the kind of investment in long-range R&D that, frankly, their missions probably demand that they do have.

And so what we took on was also the idea and we submitted this in the President's budget to, in fact, enhance those activities for Coast Guard, for example, for Secret Service, to enable them to do some of those things that might be 3 or 4 years out, that maybe we would never have budgeted for. The people who staff these positions tend to be detailees of the home organization, so they understand the culture and who to talk to and that sort of thing.

Mr. THORNBERRY. That is helpful.

If, at some point, you see an impediment in the statute to that coordination, I trust you will tell us, because that is something, obviously, that we are interested in.

Now, let me get to Mr. Etheridge's point: How do you coordinate with other departments, for example, Agriculture, on some of these diseases—but there are a lot of others, too.

Some of the information, or estimates, we have is that homeland security R&D is about one-third of that conducted by the Federal Government as a whole; so how do you do that and how is that working at this point?

Mr. ALBRIGHT. Okay. There are a couple of ways it happens.

The first and the simplest to explain is, there are formal processes that exist for interagency coordination. The White House has a couple of activities that do that. One is, the Office of Science and Technology Policy runs something called the National Science and Technology Council. It is a Cabinet level post that actually reports to the President and its primary job is to, in fact, in a variety of areas, to ensure coordination, not just in homeland security, of course, but across the spectrum of science and technology activities in the Federal Government.

Jack Marburger, over at OSTP, has been extraordinarily active in the homeland security arena; in fact, he—you know, before the Department stood up, I think the nearest thing we had to a homeland security science and technology office was OSTP; and so he has created several working groups that formalize this kind of interaction in the homeland security arena.

I happen—Chuck McQueary actually cochairs that with Mike Wynne, over in the Pentagon, and they have a number of working groups which I am heavily involved in. And so there is a formal structure.

There is also a similar structure within the Homeland Security Council in a few specific areas, but perhaps more importantly, there is an informal mechanism, and that is that we have, for example, MOUs with USDA that are formal.

We have MOUs with HHS that establish working relationships that are often required by statute; for example, USDA, we have a statutory relationship that comes about because of the Plum Island language that was in the bill. The HHS, we clearly have statutory responsibilities.

We also have responsibilities that are implied with places like NIST, we created MOUs with them.

There are also informal relationships. I happen to know all the players, and we make it our business to know each other. And Chuck McQueary, we spend time every other month over at the Pentagon; and we have shared with them our plans, they share with us their plans, and then we try to coordinate in that manner.

But having said that, can I guarantee there will never be any duplication? I cannot tell you that.

Mr. THORNBERRY. But at this stage, you feel pretty good about the level of coordination, particularly at this stage of development of the Department and your Directorate?

Mr. ALBRIGHT. Absolutely.

Mr. THORNBERRY. All right.

Let me turn to a slightly different question, but I think one that is very important, and that is the issue of metrics.

How do we measure whether we are improving, or not?

Obviously, this is something that you have to worry about to run your section of the Department. It is also something we have to worry about as we try to oversee the work of the Department, but also evaluate how taxpayer dollars are being spent.

It seems to me that particularly in the R&D world, measuring progress is a very difficult thing, so I am very—I would be very interested in suggestions you have for us and, of course, your own management on what are the sorts of ways that we can measure progress and advancement in homeland security R&D.

Mr. ALBRIGHT. That is a really interesting question.

Metrics, first of all, applied to the homeland security enterprise, writ large, are extraordinarily difficult to come up with. If you look at what our measures of effectiveness are, they tend to start with the words "prevent," "protect," and so you are proving a negative in a sense. How do you know that something hasn't happened? How is that a measure of success?

So it is extraordinarily difficult for homeland security as a whole; and as you correctly pointed out, research and development metrics are something the Federal Government has been wrestling with for a very long time.

There are ways to measure performance that are not particularly satisfying, but are perhaps better than nothing. And the first one I would offer up is—in some areas, for example, we can just count things; so, for example, we can say that we are going to issue standards, three sets of standards, standards in three areas by the end of fiscal year 2005, so we can count how many standards we have done.

The problem with that, of course, is that you start getting into counting games and what do you mean by a "count" and those sort of things.

I think the more preferred way to do it is to actually show our detailed program plans to Congress, which I like to do, and to show you the milestones we expect to achieve, both programmatic and technical in terms of performance, and when we expect to achieve them; and then I think we ought to be held accountable to those milestones. If I tell you we are going to develop a detector with this kind of performance and this kind of operation by a certain date and here is the milestone and we are going to demonstrate it, I think you have every right and should ask us, Did you, in fact, take it out to the field and demonstrate it; and what did you find out. And that is sort of the way you do it, because what that does is, it forces on us a very disciplined developmental process.

I think it is good for us that we have those kinds of way-points put in our path; and at the same time, I think it helps you feel some sense that the dollars that we are spending—which, after all, for those particular purposes, we are saying that is why we are spending them in the first place—that, in fact, some kind of progress is being made.

Mr. THORNBERRY. I think that is a good point.

I guess the only thing I would say is, I do not want you to be reluctant to set milestones and goals for fear of what happens from us if you do not meet them. I mean, understandably, there are things that happen, particularly in your line of work, but as long

as we have that communication going back and forth, it seems to me it ought to work. But I think that is very helpful.

Does the gentleman from North Carolina wish to interject on this?

Mr. ETHERIDGE. Thank you, Mr. Chairman, I would.

As it relates to this—and I think it is a great question—how does the Department determine the distribution of funds among the various R&D portfolios? And I know that has got to be difficult, as you are getting—going up and in that line, in the 2004 Homeland Security Appropriations Act, bio-countermeasures receive roughly four times the S&T funding as chemical countermeasures.

Is that because the Department views the bio-threat is four times as great, or is it based on threat? How do we determine the threat and the distribution?

Mr. ALBRIGHT. That is an excellent question, and that is—it depends on a number of things, and obviously threat is one of them.

You know, from our perspective, the threat from an anthrax attack or from a nuclear weapon is far greater than the threat from other potential things that you could imagine. So threat clearly determines a portion of our investment.

But the way we operate is—we tend to do bottoms-up budgeting, so to give you a sense of what the process is, we look at, first, the threat, and we ask ourselves, you know, what are the threats that are, you know, for example, easy to do by the bad guys and yet very catastrophic. That is probably where you want to put most of your money, okay?

So we tend to sort the threat. And then we ask ourselves, what are the activities, what are the capabilities we need to counteract that kind of threat; and we write that down, we create a strategic plan, and we, in fact, publish that. And then we ask ourselves, what program do we need to, in fact, execute that planning guidance, okay?

And that is, then, where the budget comes in and the budget constraints come in, and we sort from there. So it is a bottoms-up sort of process, and it is not correct to say that, for example, the fact that I have four times the amount in bio that I have in chem, that that is necessarily some reflection on the relative priorities, although it may be. Partially, that is true, but it is also driven by what is the right investment we need to make in each of these areas to achieve some level of performance.

What you find, for example, is, in some areas, like the bio area, there has been almost no investment in the things we need to invest in, while in the chemical area, to use your example, there has been a lot of investment made by the Defense Department over time and we are further along.

So that is how it is done, in effect.

Mr. ETHERIDGE. In light of that, the Technical Working Group has conducted a number of solicitations since 9/11 for homeland security technology proposals for those solicitations and especially the ones that were jointly done by DHS.

How many projects have been funded, if you know, and how many technologies have been fielded?

Mr. ALBRIGHT. Okay. The answer is, I do not know right now. There were several thousand proposals that we got.

Mr. ETHERIDGE. If you can just get that to us later, that will be fine.

Mr. ALBRIGHT. I will, but I do know the contracts are being let as vetted we speak.

Mr. ETHERIDGE. Thank you.

Mr. THORNBERRY. Thank you.

And before I forget it, without objection, all members will have the opportunity to submit written questions to Dr. Albright, and so we may want to follow up on some of these things, as well as, of course, present opening statements.

Mr. THORNBERRY. Let me follow up on that point, because it is, I think, a matter of interest to all Members of Congress, because we all have somebody in our district who wants to sell something. The staff had presented me with what is—as I understand, is an automated response that vendors are getting from the Department, which basically says, Go look at the Federal regulations and come back to us.

I guess I would be interested in your assessment of, number one, how this interaction with the private sector is going. And it is a very tough thing, it seems to me, because you could use all of your 150 people doing nothing but meeting with folks all day, and there may not be any of those meetings that really help the country be safer.

The other side of it is, there may be a jewel out there, and that is part of the risk I know you take; but I would be interested in how you think that communication, that contact with the private sector, is going.

I would also be interested—I think it related in TSWG and how their activities are going. Do you foresee them being a primary screening mechanism for the indefinite future?

Mr. ALBRIGHT. Okay. Let me—there are several questions in there.

Let me start with what our process is in dealing with the private sector, because that is an important point.

When we first started up the Science and Technology Directorate, there was no process within the Department at all; and so, as you recall from the May testimony, Dr. McQueary actually at that point announced, I believe, the science.technology e-mail site; and so we stood that up. And that was the—and that has gotten a lot of press, so we have got a lot of people sending material into that site.

And what we created was a process at our end for dealing with that, where we look at the submissions that come into that site—and they run the gamut, including Nigerian financial scams—we get it all in there, and we look at the kind of material we get; and truth be told, some of this—some think the queries we get there have very little detail associated with them. There is not much there to do an evaluation. Even if we had the time to do it, we cannot deal with anything.

So what we do is, we send them back actually a nice letter, telling them that there is not sufficient information here, that we will hold the application for what they have sent to us, and if they want to, you know, provide more detail, we will be happy—they should

look at other samples for what a detailed solicitation would look like.

And, by the way, everything I am talking about is unsolicited proposals, okay? If somebody brings something in that does have sufficient detail, we take them over to TSWG, okay, because they have this evaluative process in place, these groups of people who can examine and evaluate these things. They have several working groups set up. And we will inform the person who sent that thing to us that that is what we are doing, we are sending it to TSWG; and furthermore, we have a process whereby we get back to them in 30 days.

So that is the process we have set up in the Science and Technology Directorate.

So, of course, what has happened since then is, a lot of other offices, CIO shop, for example, within DHS, they too are getting hit by a lot of inquiries from the private sector, and they have created their own processes. And I guess what I am hearing from you is that we probably ought to work with those guys to try to get them the kind of robust process we have within the S&T Directorate, so that the private sector can feel they are better engaged.

How are we interacting with the private sector? I think—as I said, I think we have as good a process as you can have that balances our ability to get our jobs done while at the same time scouting and making sure that those gems do not just fall through the cracks in the pavement.

The—will the TSWG be our continued evaluative group? That is actually an open question. They may, but you have to remember, when the TSWG was formed up, it was a DOD-State entity that included Secret Service, Customs, TSA; and you sort of look at the list of agencies that comprise the TSWG, and about 90 percent of them are in the Department of Homeland Security. So one of the questions we are asking ourselves is whether or not we just want to go ahead and create, you know, our own process and, you know, work—synergize with TSWG, but at the same time not necessarily trouble DOD, for example, and trouble our working groups with, you know, technologies that have to do with new tank armor or things like that.

Mr. THORNBERRY. You may have referred to this earlier, but have you sent people over to places like DARPA, to see what they have, what plans they have that may be of interest for the Department?

Mr. ALBRIGHT. Well, yes.

Mr. THORNBERRY. Or are you waiting for them to come and say, look what we got for you.

Mr. ALBRIGHT. Well, there has been a little bit of that. I mean, I came from DARPA, as you know. That was a few years ago. As a matter of fact, our program managers within HSARPA have recently departed DARPA, very recently in many cases, so we are fairly familiar with what goes on over at DARPA.

Our interaction with the Pentagon, though, is through Paul McHale's office almost exclusively, so to the degree—I would say there is no formal interaction between us and DARPA, but we are—again, we are aware of it, but it is all through informal mechanisms.

Mr. THORNBERRY. Well, I am a little concerned, in that, for example, I have been told—and I do not know, and I need to go ask—that DARPA has done some work on designing a 21st century airport security system, using primarily off-the-shelf technology. I do not know if that is true.

I would be interested in it, but there may—not only DARPA, of course, but the Federal laboratories and other places with which you are very familiar. Sometimes it is kind of hard to root around and find some things, but there are some jewels out there, and I know none of us want them to fall through the cracks in the pavement.

Mr. ALBRIGHT. Well, I think if there is a new airport security system at DARPA, I will definitely look into that, because that is an area obviously of concern to the Department and to S&T.

As I said, there are a lot of informal mechanisms we have for dealing with DARPA in particular. There are a lot of formal mechanisms as well that deal with the Federal laboratories, and I think I mentioned those earlier.

We do work through Paul McHale in the Pentagon, and to the degree they believe the things in DARPA over at Dale Klein's shop, over at DTRA, for example, they certainly let us know.

To date, there hasn't—I have got—the airport security one is a new one on me, so—

Mr. THORNBERRY. I think it is something maybe for both of us to go check out—

Mr. ALBRIGHT. Okay.

Mr. THORNBERRY.—and I hope there is something useful for us there.

Dr. Albright, I think we continue to have a vote on the floor. I think, in light of our comings and goings, maybe we will end here.

Mr. ALBRIGHT. Okay.

Mr. THORNBERRY. But I do appreciate your willingness to provide written answers to further questions that members of the subcommittee may have, and I am very grateful for all of the communication which you and your folks have had with members of the subcommittee staff and members.

In addition to that, I want to thank the Budget Committee for letting us use their committee room and the staff for helping us hold this hearing.

Thank you. We will look forward to our continued work together to try to help the country be safer, okay?

Mr. ALBRIGHT. Thank you.

[Whereupon, at 5:42 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

QUESTIONS AND RESPONSES FOR THE RECORD

QUESTIONS SUBMITTED TO DR. PENROSE ALBRIGHT FROM THE HONORABLE JIM TURNER

1. Dr. Albright, you testified that the directorate makes resource allocations based on an assessment of the threat, and in particular the potential impact, likelihood of success, and ease of carrying out different terrorist attacks. What input do you receive from the Information Analysis and Infrastructure Protection (IAIP) Directorate in carrying out this assessment? Are you communicating with IAIP officials to get better tailored analyses?
Response: We are working closely at multiple levels with the IAIP Directorate to understand threats and vulnerabilities. This is a particularly strong connection because S&T people and capabilities are engaged in active support of the assessment functions of the Assistant Secretary for Information Analysis, particularly with regard to technical issues surrounding the threat. A joint project with the Assistant Secretary for Information Analysis is currently underway to have intelligence community resources at the national laboratories assess the weapons of mass destruction (WMD) capabilities of known terrorist organizations, and to identify information gaps that can help prioritize future analysis and information gathering. In another example, S&T was guided on longer term RDT&E priorities in counter–Bioterrorism RDT&E by working with IAIP staff in a recent workshop to determine gaps in counter–BW capabilities.

In addition, regular senior level interactions at the under secretary and chief of staff level have provided assurance since the Department's formation that threat and vulnerability related priorities are shared across DHS directorates.

2. Please provide details on the results of the Broad Agency Announcements and other solicitations conducted since 9/11 as regards homeland security and combating terrorism technologies? In particular, please indicate the number of proposals submitted to the solicitations, the number of requests from DHS and TSWG for more detailed proposals, the number of proposals ultimately accepted, the number and amounts of funds distributed to accepted proposals, and the number and names of technologies that have been fielded as a result of these processes.
Response: May 14, 2003: The Department and the Technical Support Working Group (TSWG) issued the first Department of Homeland Security (DHS) S&T Broad Agency Announcement (BAA), entitled "Combating Terrorism Technology Support Office," DAAD 05–03–T–0024, closed June 13, 2003. This BAA listed 50 requirements, sought quad-chart submissions in the first phase, and will down-select to winning proposals. There were 3,344 quad chart responses received. There were 237 white papers requested from those submitting quad charts. As of 20 November, 2003, 93 white papers have been rejected; 34 have been reviewed favorably and full proposals requested. The remaining 110 are still under evaluation. Efforts will be awarded to both private companies and government laboratories. DHS provided $30M to TSWG for awards in FY–03 and anticipates that another $30M will be available in FY–04 for this BAA. These funds are sufficient to fund the proposals already accepted and those which may be selected as the evaluation continues.

September 23, 2003: First Research Announcement (RA–03–01) for the Homeland Security Advanced Research Projects Agency (HSARPA) was issued, entitled "Detection Systems for Biological and Chemical Countermeasures Program." Its purpose is to develop, field-test, and transition to commercial production the next generation of biological and chemical detectors and systems. It addresses two areas in biological countermeasures and three areas in chemical countermeasures. The white paper deadline was October 24, 2003, and, by that deadline, 518 white papers were received. They are now entrained in an evaluation process that is on schedule to conclude by November 21, 2003. Authors of selected white papers (and other sponsors wishing to submit full proposals) will be asked to submit full proposals, which will be due December 19, 2003. Following evaluation of all proposals received, HSARPA expects to enter negotiations with selected proposers by the end of January 2004. The total amount of funds committed to this effort depends entirely on the number and cost of the proposals selected for execution.

October 3, 2003: The S&T Directorate released a solicitation (HSSCST–04–R–AR001) requesting white papers and proposals for an aggressive two-phase Systems

Development and Demonstration (SD&D) program for antimissile devices for commercial aircraft. DHS will investigate directed infrared countermeasures (DIRCM) and other technologies to provide protection against man-portable air defense systems (MANPADS). DHS does not intend for this program to develop new technologies, but rather to migrate existing technologies to the commercial airline industry. Twenty-four white papers were received and evaluated. Five teams have been asked to submit full proposals and each has been given a date during the week of December 8, 2003 to present their oral submissions. The Government anticipates selecting at least two teams for negotiation and award in early January 2004. The total amount of funds committed to this effort depends entirely on the number and cost of the proposals selected for execution.

November 13, 2003: HSARPA issued a Small Business Innovation Research (SBIR) Program Solicitation. The purpose of this solicitation is to invite small businesses to submit innovative research proposals that address eight high priority DHS requirements:

- New system/ technologies to detect low vapor pressure chemicals (e.g., Toxic Industrial Chemicals)
- Chem-bio sensors employing novel receptor scaffolds
- Advanced low cost aerosol collectors for surveillance sensors and personal monitoring
- Computer modeling tool for vulnerability assessment of US infrastructure
- Marine asset tag tracking system
- AIS tracking and collision avoidance equipment for small boats
- Ship compartment inspection device
- Advanced secure supervisory control and data acquisition (SCADA) and related distributed control systems.

The deadline for receipt of proposals is December 15, 2003. The total amount of funds committed to this effort depends entirely on the number and cost of the proposals selected for execution.

November 13, 2003: HSARPA released a Request for Information (RFI) on Radiological and Nuclear Countermeasures System Architectures Analysis (RNCSAA) Draft Statement of Work for comment (DSWC 04–01). The RFI lists four tasks:

- Develop a framework for evaluating system architectures
- Study systems effectiveness and vulnerability studies
- Define and evaluate novel architectures, and approaches for countermeasures
- Identify additional studies to support these tasks.

This RFI will lead directly to a future solicitation based on the responses to this RFI and related topics.

To date, no technologies resulting from these solicitations have been fielded.

3. What was the level of interest generated by DHS' solicitation for comments on the Homeland Security Institute RFP? What do you see as the impact on the applicant pool of the three-year sunset provision, and do you have any recommendations for changing that provision? When will the Department issue a final RFP for the Institute, and when will a decision be made on awarding a contract? Considering that the Institute is required to have expertise beyond the jurisdiction of the S&T Directorate, how will you ensure that the Institute meets the requirements set forth in the law?

What was the level of interest generated by DHS? solicitation for comments on the Homeland Security Institute RFP?
Response: The interest from all sectors—not-for-profit organizations, for-profit companies, universities, consortia, and single investigators—was high. Approximately 70 responses were received.

What do you see as the impact on the applicant pool of the three-year sunset provision, and do you have any recommendations for changing that provision?
Response: Sec 312 of the Act provides for the formation of the Homeland Security Institute, with the capability for systems analysis, risk analysis and modeling and simulation, policy analysis, support for exercises and simulations, and other activities that are traditionally performed by an FFRDC. These capabilities are in fact enduring needs for the Department that require specialized and dedicated staff focused on the broad range of issues confronting homeland security and the Department. The three year sunset clause, unfortunately, serves to discourage the acquisition of permanent staff, and the investment in resources, an organization would need to make to compete for and conduct such an enterprise. It is worth noting that Sec 305 of the Act provides also for the establishment of FFRDCs, without the three year sunset clause. Several of the more qualified potential bidders have informally

indicated that they have no interest in pursuing this contract if the three-year sunset provision is not removed. They view it as impractical to ask talented scientists and engineers and other analysts to pursue an alternative career path that will only last for a year or two. They also view it as bad business strategy to commit their own organization's resources (facilities, infrastructure, etc.) for such a short-lived commitment. In light of this, I would be happy to work with Congress to (1) remove this sunset provision entirely and allow the FFRDC to function according to normal laws and regulations that apply to FFRDCs, or (2) extend the sunset provision to 10 years, or (3) to put into effect a solution that allows the Department to overcome the difficulties created by this provision.

When will the Department issue a final RFP for the Institute, and when will a decision be made on awarding a contract?
Response: The RFP is scheduled to be released in early December, with a subsequent award in late spring/early summer.

Considering that the Institute is required to have expertise beyond the jurisdiction of the S&T Directorate, how will you ensure that the Institute meets the requirements set forth in the law?
Response: The ultimate sponsor of the Institute is Secretary Ridge and, therefore, it is viewed as a resource that will be available to the Department as a whole, although it will be managed by the S&T Directorate. The core functions—a necessary component of any FFRDC—have been carefully crafted to ensure capabilities that extend beyond just science and technology (and meet the legislative requirements). This will be one of the criteria for evaluating the proposals.

4. The PREPARE Act (H.R. 3158) has a provision that would require the Directorate to within six months identify first responder equipment and training standards that don't currently exist, and work with the standards and first responder communities to complete work on those standards within a year after that. What are the Department's plans in this regard?
Response: The S&T Standards Portfolio is working with the emergency responder organizations—Memorial Institute for Prevention of Terrorism (MIPT), and National Technology Transfer Center (NTTC), as well as the InterAgency Board for Equipment Standardization (IAB) which has a co-chair from the emergency responder community—to identify needs for standards of the emergency responders. The Standards Portfolio is also working with the Homeland Security Standards Panel (HSSP), which has been set up by the American National Standards Institute (ANSI), to coordinate development of homeland security standards among 280 standards development organizations. Work has been initiated with the Institute of Electrical and Electronics Engineers (IEEE) on radiation detector standards, with AOAC International on standards for anthrax detectors, with the National Institute for Occupational Safety and Health (NIOSH) on personal protective equipment and with ANSI on development of a database of homeland security related standards. The Standards Portfolio is engaged with the principal Departmental elements involved in training for emergency responders—the Federal Emergency Management Agency (FEMA), the Office of Domestic Preparedness (ODP), and the Coast Guard—to develop common metrics for curricula for emergency responder training.

5. The Project Bioshield plan commits NIH with doing the basic research that is necessary and obligates BioShield funds to purchase the final product from the private sector. What is the Science and Technology Directorates role in conducting the middle part of countermeasure development where research findings are converted to effective medicines. In light of the Homeland Security Act requirements that DHS and HHS will collaborate on setting priorities, goals, objectives, and policies and develop a coordinated strategy for R&D relating to medical countermeasures for terrorist threats:

How often does Directorate staff meet with NIH officials to discuss their research and development efforts? Who attends these meetings?
Response: In accordance with Section 302 (4) of the Homeland Security Act of 2002, Public Law 107–296, the Secretary, acting through the Under Secretary of Science and Technology, "shall have the responsibility for conducting basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs, except that such responsibility does not extend to human health-related research and development activities."

Accordingly, the S&T Directorate, in coordination with other DHS Directorates, identifies biosecurity threats and conducts vulnerability assessments as a basis for defining medical countermeasure priorities.

The Under Secretary for S&T, or his designees, participates on the Weapons of Mass Destruction Medical Countermeasures Working Group, co-chaired by the Department of Health and Human Services (HHS) Office of the Assistant Secretary for Public Health Emergency and Response (OASPHEP) and the Department of Defense, Assistant Secretary, Health Affairs. Three subgroups focus on Research and Development, Acquisition, and Requirements. The Assistant Secretary for S&T co-chairs the Acquisition Subgroup. The working group and subgroups provide the organizational structure to assure effective inter-agency coordination in setting medical countermeasure priorities.

In bio, chemical, and radiological defense, NIH have expanded their R&D effort to include middle and late stage development of medical products. Is the S+T directorate consulted in these programs? How is the directorate updated on what specific countermeasures NIH is actively developing and the progress of that research?

Response: In addition to the formal working groups and subgroups described in the response to the question above, the Under Secretary for S&T, or his designees, also participates in monthly risk management meetings coordinated and chaired by the HHS/OASPHEP. Representatives from the National Institute of Allergy and Infectious Diseases (NIH/NIAID), the Centers of Disease Control and Prevention (CDC), the Food and Drug Administration (FDA), as well as DHS/EP&R and S&T are active participants. Meetings are held currently on the subject of anthrax, smallpox and Botulinum toxin medical preparedness. These risk management meetings provide a forum for status reports on the progress and development of priority medical countermeasures.

How is threat assessment or the needs of first responders, as determined by DHS, being integrated into prioritization for medical countermeasures R&D?

Response: The S&T Directorate has chartered and is working very closely with the HHS, as one of a number of federal organizations, to conduct of technical threat assessments of current and future biothreat agents and to develop processes to conduct systematic vulnerability assessments. The results of periodic threat and vulnerability assessments will be communicated to the Weapons of Mass Destruction Medical Countermeasures Working Group and additional agencies as appropriate.

I understand that Dr. Michael Ascher is the Directorate's senior medical advisor. What is his role? To whom does he report?

Response: Dr. Michael Ascher was the Senior Medical Advisor for the Biological Countermeasures Portfolio until his return to California this summer. Dr. Peter Estacio is in the process of joining us to fill this role. The Senior Medical Advisor reports directly to the Portfolio Manager for Biological and Chemical Countermeasures (Dr. John Vitko) and is responsible for interacting with the biomedical countermeasures community, assessing the current status and any gaps as they pertain to overall biodefense, and guiding the Portfolio and DHS S&T activities appropriately.

QUESTIONS SUBMITTED TO DR. PENROSE ALBRIGHT BY CHAIRMAN THORNBERRY AND THE HON. ZOE LOFGREN OF THE HOUSE SELECT COMMITTEE ON HOMELAND SECURITY

Questions from Representative Dunn

1. In your testimony, you explain that the S&T Directorate is helping the Information Analysis and Infrastructure Protection (IA&IP) Directorate develop the technological ability to map vulnerabilities within the oil and gas infrastructure in the Southwest states. I am particularly interested in this issue because of a pipeline explosion in 1999 that killed three children in my home state of Washington. Is this mapping going to be done in other regions—in addition to the Southwest? Have you had success working with the private sector on this project so far?

Is this mapping going to be done in other regions—in addition to the Southwest? Yes. Our Critical Infrastructure Protection (CIP) Decision Support System (DSS) project supports the IAIP Directorate to understand the functions and vulnerabilities of all of the nation's 14 critical infrastructure sectors and key assets as well as the interdependencies among them. We have developed modeling and simulation capabilities at the national level as well as at the regional and metropolitan level.

Have you had success working with the private sector on this project so far?

Yes. The team of Department of Energy (DOE) laboratories that is developing the CIP–DSS for us has collaborated and worked for years with most of the major oil and gas associations in addition to numerous private companies and utilities. The associations include the American Gas Association (AGA), Interstate Natural Gas Association of America (INGAA), American Petroleum Institute (API), and the Gas Technology Institute (GTI). They have also worked with Olympic Pipeline (BP), Kinder Morgan (an integrated liquids pipeline and storage company), Conoco, and many of the largest natural gas utilities in the US.

2. I was pleased to read in your prepared statement about how much the S&T Directorate has achieved—and I am also pleased that you believe long-term research must be a priority as we move forward. Do you feel you have the resources you need to carry out your mission on a day to day basis? Are there specific areas that you would like this committee to focus in on in the future that have not, in your opinion, received the attention they deserve?

The Science and Technology Directorate has reviewed its authorized fiscal year 2004 funding and its proposed fiscal year 2005 funding and presently believes the current and proposed funding is adequate. However, we continue to assess our research and development plans. If we determine that the proposed amount of our funding is not sufficient to meet requirements, we would bring that information forward for consideration through the appropriate mechanisms. Additionally, in order to accurately determine what level of funding is needed for our research, development, testing and evaluation (RDT&E) activities, we will continue to work with other agencies with R&D responsibilities to identify requirements and gaps in funding. This coordinated approach will assist in making the right investments while preventing unnecessary and wasteful duplication.

The Science and Technology Directorate recognizes there are some technology needs that require immediate attention. However, some homeland security issues require basic research to solve. Our long-term portfolio plans will address basic research needs.

3. I have spent a considerable amount of time learning about a variety of homeland security-related technology being developed by some of my constituent companies in Washington State and I?m sure most of the other members of this committee have done the same.

I am wondering how your directorate is working with other directorates to ensure that the technologies being used for different functions within the Department are the best we can get, and will be most effective in waging the war on terror here at home, and will lead to greater coordination among directorates?

Coordination among directorates is a top priority of the Department of Homeland Security (DHS). We have regular senior level management meetings to identify issues and share information that cross-cuts the Department. Once a week, a teleconference is held with representatives from all the components of the Department. This meeting ensures that personnel from each of the Directorates become familiar with personnel from the other Directorates to facilitate intradepartmental communication. In addition, a number of Science and Technology (S&T) Directorate staff sit on interagency working groups with staff from other directorates. Within the S&T Directorate, we have portfolio managers for Border and Transportation Security, Emergency Preparedness and Response, United States Secret Service and United States Coast Guard. These portfolio managers serve as liaisons to the other components of the Department and ensure that we are supporting their operational needs. The S&T Directorate is also responsible for developing standards related to technologies that DHS is creating or applying, and, through this function, the S&T Directorate makes sure that equipment and technologies are as effective as possible.

What is the best way for a business to bring an idea to the attention of your office? How are those proposals currently being evaluated?

The best method is to read carefully DHS solicitations for technology concepts and ideas that are posted at http://www.fedbizopps.gov and on the DHS public website, http://www.dhs.gov. DHS is interested in pursuing technologies posted in these formal, public, competitive solicitations and has budgeted funds for awards to the most meritorious submissions.

If a business has an idea or concept that does not addresses a specific requirement in one of our active solicitations, we invite them to contact the appropriate Program Manager (PM) within our Homeland Security Advanced Research Projects Agency (HSARPA) by telephone or e-mail for an initial discussion of their idea. Contact information for these managers will be listed on the DHS public website

(www.dhs.gov) shortly. If the proposed idea seems to match a DHS need, the HSARPA PM will ask them to submit a brief white paper. If after review of the white paper, the approach still looks good, the Program Manager will suggest that the business consider submitting a complete proposal. A brief listing of the HSARPA Program Managers and their contact information is attached for information.
White papers should contain a top level summary of the concept; a clear description of the underlying principles and concept of operations; the current state of development of the key technologies proposed; identification of critical path technologies and the approach to ensuring that these will be sufficiently mature to meet development deadlines; an estimate of the funding level required in each year; a summary of related technologies and/or systems previously developed by the proposed team; and a brief description of the qualifications of principal team members. White papers are typically 5–10 pages in length.

The address for submitting the information is:

Department of Homeland Security
Attn: Science & Technology Directorate/Program Manager's Name/Room
Washington D.C. 20528

or, they may be submitted electronically to:

http://www.science.technology@dhs.gov

If businesses so choose (especially with those applications they think are nearest term and most useful), they may submit a complete unsolicited proposal.
Part 15.6 of the Federal Acquisition Regulations, available on-line at http://www.arnet.gov/far, specifies the few criteria and a nominal submission format for unsolicited proposals. If this format is followed, all the required information will be at hand to evaluate the proposal. These unsolicited proposals should be submitted to the addresses listed above.

In evaluating responses to published solicitations, the evaluation criteria are always published in the solicitation. The proposing business should always read the solicitation carefully and match their proposal to the content and format requirements.

4. I would like you to expand on the subject of Man Portable Air Defense System (MANPADS)—you included in your testimony a brief description of your directorate's R&D program to understand both the threat posed by man-portable missiles and the technology that is available to address the threat. What is the department doing to analyze the threat from other ground-based weapons to the commercial aviation system—such as non–Infared (IR) guided missiles and propelled grenades, for example? Is the department taking a systematic and risk-based approach to create a comprehensive, efficient response to ALL of these threats?

The Department of Homeland Security's Science and Technology Directorate maintains close coordination with the Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), Transportation Security Administration (TSA) and Department of State (DoS) representatives to remain abreast of all current and emerging ground-based threats to commercial aviation. After reviewing intelligence analyses from agencies such as DIA's Missile and Space Intelligence Center (MSIC), a systematic, end-to-end countermeasures strategy is formulated, and a program is implemented to mitigate risks from the threats. The strategy focuses on three areas. DoS is mitigating risks from these terrorist threats through proliferation control and threat reduction. TSA is utilizing tactical measures to address airport vulnerability, perimeter security and other countermeasures working with law enforcement agencies. Based on these assessments, the S&T Directorate identifies the critical threats, analyzes the susceptibility and vulnerability of civilian aircraft to them, and formulates technical solutions necessary to counter these threats.

Questions from Representative Weldon

1. The adoption of standards and certification criteria for training, equipment and protective clothing should be one of the highest priorities for DHS. The reason for this importance is that manufacturers are hesitant to invest in the development of new technologies due to a fear that the government may subsequently find that they do not meet desired needs or specifications. Furthermore, public safety agencies are hesitant to acquire new technologies due to a fear that they will be denied compensation with homeland security funds. Meanwhile, valuable solutions to homeland security obstacles are available with no clear vision of when they will be taken advantage of. For these reasons, the desires of the Department must be made clear in the form of standards. Can you please explain the Depart-

ment's plan and timeframe for the eventual adoption or creation of standards and certification criteria?
We agree that adoption of standards and certification criteria for training, equipment and protective clothing for emergency responders is one of the highest priorities of the Department. The responsibility for DHS standards is assigned to the Science & Technology Directorate. An Office of Standards has been set up that reports to the Assistant Secretary, S&T Directorate, and this office is working with the emergency responder communities and the private sector consensus standards development organizations to adopt existing standards that are appropriate, to identify needs for new standards, and to set up writing groups of experts drawing on the existing standards efforts at the Federal, state, and local levels and in the private sector. The S&T Directorate is working closely with the American National Standards Institute (ANSI) in support of their Homeland Security Standards Panel. ANSI is proving to be an effective partner with DHS in identifying appropriate standards development organizations in different homeland security technologies. The adoption of existing standards has already begun and certification criteria for laboratories are being developed that will leverage existing public and private sector laboratory accreditation organizations.

2. Many believe that the government should not be the entity that writes standards. Instead, they favor the government shaping them and even adopting them, however the actual drafting should be left to the industry and voluntary consensus process that has worked so well for first responders for many years. The National Fire Protection Association (NFPA) is a noticeable leader in the creation of codes for training and technology, which have been in place for many years. In addition, the voluntary consensus standard process is an effective and quick process involving the private industry, agencies, users and code writers, which is ever evolving and used successfully in the Assistance to Firefighters Grant Program. Does the Department intend to draft new standards or does it intend to adopt those already in existence by the private sector and first responders?
The Department supports use of the Voluntary Consensus Process. The Department recognizes both the need and the value in developing voluntary consensus standards as required by the National Technology Transfer and Advancement Act (PL 104–113). The emergency responder communities—fire fighters, HAZMAT and EMS teams—must be directly involved in the standards development process. The Department is supporting the excellent standards development for fire fighting equipment and training by the National Fire Protection Association (NFPA). The S&T Directorate is working with NFPA and the Congressional Fire Services Caucus to announce five NFPA standards that will be immediately adopted by DHS for homeland security applications. DHS is also supporting standards development at the National Institute for Occupational Safety and Health (NIOSH) as well as research to develop next generation protective equipment at the North Carolina State University. Both NFPA and NIOSH will be involved in developing DHS standards for this next generation of personal protective equipment.

Questions from Representative Gibbons
1. Part of the S&T Directorate's responsibility is to unify and coordinate much of the federal government's scientific efforts including national laboratories and academic institutions. While scientific research in academic settings can be used to thwart attacks by our enemies, it can also be used by our enemies to attack us, since much of the information is published openly. In January of this year, you spoke about "scientific Openness and National Security." One of the problems you noted in your speech was that the scientific community has not established any real, unified criteria for the open publication of sensitive scientific research. You specifically referenced the public release of a Mouse Pox study and a Polio Virus study and how those could have harmed our national security. Could you briefly discuss—- first, how you now view this tradeoff between scientific openness and national security and—- second, while you have stated that you believe the federal government should not be setting limitations on openly published scientific works, I wonder how you would view a coordinated effort by the National Academies or similar entity to set the standards.
The tradeoff between scientific openness and national security is, and will continue to be, a delicate balance for all federal agencies that support scientific research at our nation's universities and national laboratories. Similar concerns exist within the private sector. The Department of Homeland Security remains committed to preserving the academic freedom and integrity that have made our nation's higher education system the envy of the world. However, the nation cannot risk the protection

of our homeland under any circumstance, including the publication of sensitive homeland security information. The balance between scientific openness and national security can only occur through open and ongoing communication between the federal entities that support federally-funded research and development and the performers. I continue to encourage the scientific community to establish unified criteria for open publication of sensitive scientific research and I am committed to engaging with all the scientific community as we address this issue.

DHS would welcome the continued, thoughtful participation of the National Academies in formulating guidelines to assist federally-sponsored research organizations in the determination of how best to safeguard sensitive homeland security information. The recent National Academies report, Biotechnology Research in an Age of Terrorism, considered the question of scientific openness and national security in the realm of biotechnology research. The report is extremely valuable and had several worthy recommendations, including the need for the education and involvement of the national and international scientific societies and associations in this important issue. In addition, the report recommended that scientific societies that publish research results establish a system for effective self-monitoring of information that may be considered sensitive to our national security.

2. You mentioned that the Defense Advanced Research Projects Agency (DARPA) and the Homeland Security Advanced Research Projects Agency (HSARPA) have different missions and responsibilities. However, I can imagine several areas of research that could be mutually beneficial to both homeland security and defense. Do you believe that HSARPA and DARPA are in a good position to work together to take full advantage of each others' work? If so, what is the formal mechanism for this co-operation?

DARPA and HSARPA are well positioned to work together. They share mutual interests in technologies related to Homeland Security missions. For example, they are now collaborating on a $10 million joint radiological decontamination research effort under the terms of a formal Memorandum of Agreement signed by both Directors. Some of the original HSARPA Program Managers are DARPA alumnae and maintain their professional ties and relationships. The Directors of the two organizations are in frequent contact and the immediate past Deputy Director at DARPA is HSARPA's current Deputy Director. At this time, DHS does not feel the need for a formal agreement to further structure this close working relationship.

Questions from Representative Langevin

1. I know the University of Rhode Island is putting together a white paper on its vision of what a DHS Federally Funded Research and Development Center (FFRDC) should be and how it should be organized. How will the FFRDCs fit into DHS's overall research framework and goals? Can you tell us if the Directorate is anywhere near a decision on what their purpose and goals will be? Since the call for white papers is ending, when do you anticipate a request for proposals to be made? Will you ask Congress to increase the authorization period for this FFRDC (currently only 3 years), especially since it has taken so long to start the process of establishing it?

The Homeland Security Institute (HIS), a Federally Funded Research and Development Center, is being established under the authority of Sec. 312 of the Homeland Security Act of 2002 to provide research, studies, analyses, analytic and computational models, simulations, and other technical and analytical support to the Department. The HSI will adopt an integrated systems approach to evaluating homeland security systems and technologies at all stages of development, deployment, and use.

A request for proposals was issued on December 3, 2003, with proposals due on January 28, 2004. The expected award date is May 1, 2004. The initial award will be $8.5 million in fiscal year 2004 followed by four additional option years projected at $30 million per year. However, legislation calls for the HSI to terminate November 2005. Although the contract will be designed to accommodate work beyond that date, either legislative authorization (the most desirable approach) or a completely new FFRDC justification will be needed to extend the operations beyond November 2005.

2. I recently conducted a survey in my district of local officials and first responders, asking their opinion on homeland security concerns. Overwhelmingly, they have said that there is far too little information being shared by DHS with local officials, and this is hampering their efforts. I know they aren't alone, and I am sure that this is a concern every Member shares. What progress has been made on the information sharing standards that the Directorate was charged with developing? I know a big part of the

concern revolved around security, so I?m curious to know if the work has been passed to National Institute of Standards and Technology (NIST), or is it being handled by DHS? Is there a timeline that is being followed or a deadline for adoption and implementation?

The Department of Homeland Security believes that this request requires several responses to understand the Department's initiatives to assist the first responders regarding access to information, intelligence, and standards.

DHS has several programs in place to aid in the identification, selection, and implementation of equipment and technology for first responders:

Through the Memorial Institute for the Prevention of Terrorism (MIPT), the Department has engaged in a research effort designed to improve local, state and federal emergency responders' capabilities to deter or mitigate terrorist use of chemical, biological, radiological, nuclear or explosive/incendiary (CBRNE) devices and emerging threats. This effort has two major components:

1. The development of the architecture for an automated knowledgebase that provides responders and planners information about what technologies are already available, the extent to which they have been tested, the standards they meet, their consistency with the Interagency Board's Standardized Equipment List, and reviews from other responders that have used them. The Responder Knowledge Base became accessible this fall and although it has limited information it has been well recived by the community and new products are being added requlary.

2. The development of a national technology planning process that:

- Identifies and prioritizes the capabilities emergency responders need.
- Identifies what technologies are required to enable those capabilities, and characterizes the extent to which these are already available.
- Establishes technology objectives and roadmaps by which Federal RDT&E investments can be focused towards the needs of responders.

In addition to the MIPT programs, DHS in response to Section 313 of Public Law 107–296 of its authorizing language is developing a technology clearinghouse, the Public Safety and Security Institute for Technology (PSITEC). The mission of PSITEC is to enhance public safety and security through the identification, development, and distribution of integrated technology, programs, and information. PSITEC will serve as the single point of entry to relevant public safety information such as:

- access to and dissemination of information regarding commercially available products and innovative technologies including performance capabilities, training requirements to implement and sustain the equipment, and the availability of grant programs to facilitate the acquisition, deployment, and maintenance of the equipment,
- provide support to individuals seeking guidance on how to pursue proposals to develop or deploy technologies that would enhance homeland security,
- collect information about critical incident response training programs and develop a searchable data base that will aid responders in identifying, comparing and selecting the appropriate training courses, and
- development of expert/mentoring systems and information retrieval and analysis programs to coach first responders through their online searches of existing databases for clear and comprehensive information about equipment, programs, training, and funding.

Information sharing with state and local officials is also a top priority for the Department. In particular, both our Office of State and Local Government Coordination (OSLGC) and the IAIP Directorate are focused primarily on finding ways to improve information sharing.

State and local homeland security officials already have a seat at the table, and are both providers and recipients of homeland security information. For example, the Administration's Homeland Security Advisory Council has a State and Local Senior Advisory Committee and a First Responder Senior Advisory Committee, which facilitate communication among states and localities on homeland security issues. In addition, we regularly form ad hoc state and local advisory groups to assist in the development and implementation of homeland security policies. Finally, the Office of State and Local Government Coordination regularly consults with state and local officials as well as the major associations that represent them through publications such as DHS Today, Fact Sheets and Press Releases. Feedback from our state and local constituency indicates that these improvements are making a difference.

The OSLGC in conjunction with the rest of DHS has made major strides, since its creation, to share information with states and localities. The OSLGC is responsible for sending out homeland security information bulletins and alerts, including a daily Homeland Security Operations Morning Brief. The OSLGC also coordinates bi-week-

ly conference calls with all of the Homeland Security Advisors in all the states and territories to help relay important departmental information as well as respond to queries from the advisors.

Through the coordination of the OSLGC, the Department has paid for and established secure communication channels to all of our state and territorial governors and their state emergency operations centers. This investment in communication equipment included secure video teleconferencing equipment along with STU/STE telephones. In addition, we have worked to ensure every governor has been cleared to receive classified information and are working with the Governors and their Homeland Security Advisors to provide security clearances for five additional people who support the Governors? Homeland Security mission. Finally, OSLGC coordinates resource deployment to state and local governments, including BioWatch, air assets and radiological detection pagers, to name just a few.

To address first responder requirements regarding communications interoperability, SAFECOM serves as the umbrella program within the federal government to help local, tribal, state, and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications. To successfully achieve its vision, SAFECOM is working with existing federal communications initiatives and key public safety stakeholders to address the need to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks.

SAFECOM is a public safety practitioner driven program, and as such, solicited information from representatives of public safety from the local, state, and Federal level in establishing the program's short and long-term initiatives. Two of the top priority initiatives that this diverse group emphasized to SAFECOM include 1) the need for an "information clearinghouse" to enable two-way communication with public safety and 2) the development of a process to advance communications equipment standards. The portal, which is scheduled for release in the summer of 2004 and which will be accessible at www.safecomprogram.gov, will provide public safety practitioners with planning and management applications, collaborative tools, and relevant and timely wireless information. SAFECOM's activities in terms of standards will be to identify, test, and, where necessary, develop standards in coordination with the public safety community and ongoing standards activities.

Finally, the Department has implemented a standards development program. Working with the private sector through the American National Standards Institute (ANSI) and its Homeland Security Standards Panel (HSSP), DHS is identifying existing standards that can be adapted for homeland security needs. The HSSP is working to mobilize the resources of 280 standards-development organizations that develop voluntary consensus standards for products and processes. The Department is also working directly with the National Institute of Standards and Technology (NIST) on development of new standards for personal protective equipment for first responders, as well as standards for detectors for weapons of mass destruction and information technology standards for cyber security and for biometrics. To compliment it's standards development program, DHS plans to implement a standards based test and evaluation process to ensure that commercially available equipment performs as intended and meets the operational requirements of the first responders.

3. From all indications, identification of critical infrastructure seems to be taking far more time than was anticipated. Does DHS have sufficient capability to accomplish this task? Are you actively working on new methodology to enhance and speed-up this process?

Does DHS have sufficient capability to accomplish this task?

Yes, but it is important to put this task into perspective. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Feb 2003) identifies 14 critical infrastructure sectors and key assets. The National Strategy also provides a sense of the magnitude of the task of identifying what is really critical from the following example sites; the United States has:

- 1,912,000 Farms
- 87,000 food-processing plants
- 1,800 federal water reservoirs
- 1,600 municipal waste water facilities
- 5,800 registered hospitals
- 87,000 emergency services entities
- 250,000 firms in the Defense Industrial Base
- 2,000,000,000 miles of telecomm cable
- 2,800 electric power plants
- 104 commercial nuclear power plants

- 300,000 producing oil and natural gas sites
- 5,000 public airports
- 120,000 miles of major railroads
- 590,000 highway bridges
- 2,000,000 miles of pipelines
- 500 major urban public transit systems
- 26,600 FDIC-insured banks and financial institutions
- 66,000 chemical plants
- 137,000,000 postal and shipping delivery sites
- 5,800 historic buildings
- 80,000 dams
- 13,300 federal government owned/operated facilities
- 460 skyscrapers

The Information Analysis and Infrastructure Protection (IAIP) Directorate is working very hard with the infrastructure owners and operators to identify the most critical sites and reduce their vulnerabilities. Progress has already been made in identifying nationally critical assets. For example, for the approximately 590,000 highway bridges, the U.S. Coast Guard (USCG), the Federal Highway Administration (FHWA), and the American Association of State Highway and Transportation Officials (AASHTO) compiled "short lists" after September 11, 2001. The Transportation Security Administration (TSA) then used these "short lists" as starting points for applying the criticality model. To date, the criticality model has been applied to approximately 15% of the nation's transportation infrastructure.

Are you actively working on new methodology to enhance and speed-up this process?
Yes. Our Critical Infrastructure Protection (CIP) Decision Support System (DSS) project supports the IAIP Directorate to understand the functions of all of the nation's 14 critical infrastructure sectors and key assets as well as the interdependencies among the sectors. We are developing modeling and simulation capabilities for the analysis of threats, vulnerabilities, and consequences (risk) at the national level as well as at the regional and metropolitan level. This capability will help us more rapidly set risk-based priorities, identify critical nodes, and understand interdependencies that may change the priorities. In addition, we have initiated a university-based research and development center at the University of Southern California that will help DHS better understand and manage risk and the economic impacts of our actions and policies.

4. DHS was given broad research capabilities by the Homeland Security Act, how much are those assets being utilized?
The two most prominent research capabilities granted to HSARPA were the ability to use Other Transactions Authority for Research and Prototypes (OTA) to facilitate award of contracts, and the Section 1101 Experimental Personnel Management Program to hire skilled program managers.
HSARPA's first major solicitation to private industry sought ideas, concepts and technologies for the next generation of chemical and biological sensors. As was the explicit intent, HSARPA expects to award winners of this solicitation using OTA. This powerful tool allows companies that have never done business with the government before the opportunity to participate with an absolute minimum of red tape. OTA will be used to create an appropriately flexible program management structure tailored to program development needs.
The Section 1101 Experimental Personnel Management Program authority has been used to hire three program managers and is the preferred method for a fourth prospect. The authority was essential to recruiting and hiring these experienced technical program managers. Section 1101 completes the toolkit for HSARPA hiring of program managers. With four methods available to secure services of qualified and experienced program managers, (i.e., direct government hire, detail from another government agency, Inter–Governmental Personnel Act hiring authority and Section 1101), HSARPA has the flexibility and authority it needs to hire, retain, and rotate excellent personnel. Under the provisions of the law, HSARPA is required to report to the Congress annually on its use and progress using this authority. The first report was submitted 16 October, 2003.

How close is DHS in choosing a National Laboratory to carry on a good deal of its pure research initiatives? What about the selection of the University Centers, what is the plan for their selection? What focuses do you envision them having?
The homeland security capabilities at all the Department of Energy national laboratories, technology centers, and sites are important and vital resources to the S&T Directorate. It is essential that the nation's best and brightest scientific and technological expertise be engaged in the homeland security mission. The S&T Directorate

is committed to utilizing the extensive capabilities of all DOE national laboratories to protect the homeland.

We are implementing separate mechanisms to access the capability base at the DOE national laboratories to guard against organizational conflicts of interest and inappropriate use of inside information in responding to competitive private sector solicitations. The S&T Directorate has designated five national laboratories (Lawrence Livermore, Los Alamos, Oak Ridge, Pacific Northwest and Sandia) as intramural laboratories; all other DOE laboratories, sites and technology centers are designated as extramural laboratories. The DOE national laboratories designated as intramural labs will help the S&T Directorate set research goals and requirements and formulate research and development road maps; this level of engagement gives the intramural labs unfair advantage, were they able to compete for funding awarded through open solicitations. All extramural laboratories can compete for open solicitations from the S&T Directorate..

5. If DHS is focusing far more on near-term projects than long-term research, shouldn't there be better utilization of the TSWG, focusing more of DHS' research funding there?

The S&T Directorate does not focus on the concept of near-term and far-term research as categories; rather, we seek to place the priority emphasis on meeting the technology requirements of first responders and DHS operational users in the field. Our work here must be first rate and get the technology out to the users as rapidly as possible. This effort involves improvements, modifications, cost reductions, rapid prototyping and other development work that is innately of shorter duration. We place a parallel, but necessarily smaller, emphasis on revolutionary technology and longer term directed research.

Revolutionary technology, if successful, upsets asymmetric advantages of the terrorists, re-writes technological rules of engagement substantially in our favor, or provides an individual, breakthrough capability that creates new, major operational advantages for our people. Revolutionary research provides opportunities to explore novel solutions, try multiple technical approaches to a problem, revisit abandoned techniques in light of new progress in other areas, and is the only opportunity to "swing for the fences." It is not "curiosity-based" research, it is mission-based research, but with adequate resources and opportunity to conceive new ideas, stretch existing concepts, and cut new paths toward a solution. These clearly are the efforts that permit breakthrough capabilities to emerge, and every dollar spent in this pursuit is worth it.

DHS provided $30 million in fiscal year 2003 and fiscal year 2004 to the interagency Technology Support Working Group (TSWG) to fund awards from our first joint Broad Agency Announcement. This Announcement contained 50 requirements in which both DHS and TSWG had interest. Because HSARPA Program Managers are members of the TSWG working groups and the Director of HSARPA sits on the TSWG Executive Committee, we are closely allied and understand their operations, funding, evaluation criteria, and management.

However, there continue to be areas where DHS requirements and TSWG requirements differ substantially. Where our interests coincide, we will be active funders and participants in the TSWG processes and solicitations. Where our requirements and theirs diverge, we retain the ability to solicit and develop precisely what our clients have requested. Specifically, the requirements for volume commercial manufacture and application at affordable cost often differ from requirements typically given TWSG by their sponsoring organizations.

6. What is the status of the HSARPA? If its goal of near-term projects is similar or identical to TSWG's, why are we funding a duplication of efforts? How much project money has gone into HSARPA this year, and how does that compare to TSWG?

HSARPA was established effective March 1, 2003, with the other components of the S&T Directorate and the Department. It is active and growing. Congress established HSARPA to "promote revolutionary changes in technologies that promote homeland security," to advance those technologies which are "critical," and to "accelerate the prototyping and deployment of technologies" that reduce homeland vulnerabilities. HSARPA performs these three functions by awarding procurement contracts, grants, cooperative agreements, or other transactions for research or prototypes to public or private entities, businesses, federally funded research and development centers, and universities. HSARPA is an external funding arm for the Department of Homeland Security's Science and Technology Directorate.

TSWG focuses on short-term projects of interest to multiple agencies. Staff members from HSARPA, other S&T Directorate personnel, and representatives from other parts of DHS participate in the TSWG requirements setting process.

However, because TSWG's core funding comes from DoD, and its staff are DoD personnel or contractors, their requirements list is heavily weighted with projects of multiple agency interest that are also of DoD interest. Many topics of interest to DHS do not rank highly in the TSWG process. In other areas, there may be interagency interest in general, but a specific requirement of DHS (e.g., cost of ownership, time of delivery) necessitates that HSARPA create and manage a project to accomplish that goal. The TSWG process allows DHS to leverage its money in those areas that are appropriate for interagency work. In other areas, it is appropriate for HSARPA to compete proposals to satisfy DHS requirements. A final control on preventing inappropriate duplication of efforts is that the Director, HSARPA sits on TSWG's Executive Committee and is thus able to identify and resolve potential areas of overlap between HSARPA and TSWG.

Using fiscal year 2003 and fiscal year 2004 funds, HSARPA expects to award contracts exceeding a total value of $300 million to perform and support its research activities. TSWG receives a core budget from the Department of Defense of approximately $50M. When member contributions are included, as well as other participating support from the Department of Energy and Department of State, TSWG projects that its annual fiscal year 2004 budget will reach $160M.

Questions from Representative Thornberry

1. The intent of the SAFETY Act is to remove liability and risk barriers to the deployment of anti-terrorism technologies so such technologies can be much more widely used to protect our citizens. Even companies that have obtained some insurance to cover liabilities associated with their anti-terrorism technologies may be prevented by liability and risk barriers from obtaining additional insurance and deploying such technologies as widely as they and potential additional customers would like. Is it the Department's understanding designation and certification under the SAFETY Act can be granted to entities that were able to obtain limited insurance (thus allowing a limited distribution of their anti-terrorism technology) but whose global liability exposure prevented that entity from obtaining additional insurance (thus limiting the distribution of its anti-terrorism technology to less than all who might benefit from it)?

Yes, it is the Department's understanding that, if all of the criteria set forth in the Act for Designation and Certification are met by a Seller's technology, and if the price of the liability insurance can be shown to be preventing the technology from reaching the appropriate market, then the ability of a Seller to obtain insurance at the higher level will not prevent the Department from granting a Designation.

2. How are technical standards being established and enforced across the Department for cybersecurity, law enforcement or counterterrorism? Who set the requirements and how are they communicated to the technology developer or purveyor? Will there be a test bed(s) established to assure that technologies meet the standards as claimed?

Technical standards for products, services and systems are being developed in the Office of Standards in the DHS S&T Directorate. Many of the 22 agencies that were combined into the new Department have standards programs for products and services. These included cyber security requirements for which agencies follow regulations in the Federal Information Security Management Act (FISMA). These component agencies continue to use Federal Information Processing Standards (FIPS) as well as National Institute of Standards and Technology (NIST) guides for computer security (NIST 800 series guides). A common policy for standards for cyber security is being developed by the S&T Directorate, the other three directorates, and the office of the Chief Information Officer In the area of technical standards to support law enforcement, DHS is focusing on the technology requirements of emergency responders—including law enforcement personnel—in several areas including detectors for CBRNE agents, personal protective equipment, urban search and rescue robotics, and interoperable communications equipment. Performance specifications are being developed by consensus committees who include emergency personnel as well as equipment manufacturers. The Department is also establishing performance specifications for CBRNE detectors for use by federal, state and local personnel. Manufacturers are involved in the working groups to develop these performance standards.

In each of these areas, test beds are being established for Test & Evaluation (T&E) against the performance specifications developed by the S&T Office of Standards.

T&E protocols are being developed for use at these test beds. T&E protocols will be provided to both private sector and federal test beds. Federal test beds are being established to allow specialized T&E for select agents and for other T&E that must be conducted in a secure environment.

3. How can the certification process as required by the SAFETY Act be accomplished when standards have not yet been set for technologies seeking certification? How will these two processes be integrated? Will technologies that may be certified, have to be recertified if new standards substantially affect product acceptability?

The Department will use any existing standards that are directly relevant to that anti-terrorism technology, as deployed in a mass loss scenario, to assist in assessing the merit of any technology regarding SAFETY Act Certification. However, the Department anticipates that many of the technologies that the nation would most benefit from granting SAFETY Act protections will be cutting-edge, high-risk, high-benefit anti-terrorism technologies. Also, the term "technology" as used in the SAFETY Act is extremely broad. It includes not only devices, but also systems and services. As such, it is unlikely that applicable standards will yet exist. However, these technologies may address critical and time-sensitive needs. Therefore, we will be using additional methods to assess technology performance.

Certification as required by the SAFETY Act relies on the ability of a technology to meet all of the seven criteria required for Designation, as well as the additional criteria for Certification. Surrogates for meeting a standard are interpreted as those Designation criteria set forth in the Act as:

- "Prior US government use or demonstrated substantial utility and effectiveness," and
- "Evaluation of scientific studies that can be feasibly conducted in order to assess the capability of the technology to substantially reduce risks of harm"

For Certification, a technology also must be shown to:

- Perform as intended
- Conform to the Seller's specifications, and
- Be safe for use as intended

SAFETY Act technical review teams will rely on existing technology performance tests and analyses provided by the Seller. The teams will also draw on their own expertise and any similar evaluation information to evalute the information provided. The Office of Standards within the S&T Directorate will work with SAFETY Act teams to identify appropriate standards and Testing and Evaluation capabilities as needs are identified. As accredited certification laboratoriess are established, the SAFETY Act Office will direct those Sellers with insufficient evidence of performance to those labs as one alternative to addressing the criteria

4. After we make the investment in R&D for new technologies and follow-on test and evaluation, how is the Directorate going to assure the technologies are going to be used?

The Science and Technology Directorate will assist industry in getting their technologies (as long as they meet DHS standards) in front of operational users, including first responders. However, it is outside the scope of the S&T Directorate to guarantee that particular technologies will be selected and procured by operational users.